Centre for Information Policy Leadership
Hunton & Williams LLP

Vigilar en Busca de Resultados

Estrategias y prioridades para promover el Liderazgo y la construcción de relaciones efectivas

Artículo de discusión

10 de octubre de 2017

Contenidos

Diez Preguntas para la Discusión

"Vigilar en Busca de Resultados" involucra tomar decisiones difíciles, pero esenciales, sobre estrategias y prioridades. Las Autoridades de Protección de Datos (APDs) simplemente no están en capacidad de hacerlo todo, así que se requieren decisiones estratégicas sobre qué funciona mejor.

1. Cuando los retos y las expectativas de la era digital son tan grandes, y especialmente cuando los recursos son limitados ¿cuáles son las mejores formas para que las APDs (de forma independiente y con otros), se aseguren de que la vigilancia en datos personales produzca los mejores resultados?

2. ¿Qué caminos se deben explorar para incrementar los presupuestos de las APD a niveles más realistas?

3. ¿Qué se puede aprender de las aproximaciones adoptadas alrededor del mundo en otras esferas regulatorias?

4. ¿Puede elaborarse sobre el concepto de efectividad en términos de permitirle a los ciudadanos desarrollarse con dignidad y autonomía en un mundo digital donde se previenen los usos inaceptables de datos personales?

5. Cuando las responsabilidades de la mayoría de las APDs son tan numerosas, ¿cuáles son las mejores formas de alcanzar una efectividad real?

6. ¿La Aproximación Basada en Resultados ofrece formas útiles para establecer prioridades estratégicas y para alcanzar un balance entre relacionamiento, sanciones y gestión de quejas?

7. ¿Es correcto darle una prioridad estratégica de alto nivel a las funciones de liderazgo con un énfasis fuerte en el relacionamiento constructivo con los sujetos vigilados?

8. ¿Qué actividades y técnicas pueden promover mejor un relacionamiento constructivo en la práctica?

9. ¿Los organismos que coordinan a las APDs a nivel global, regional y operacional considerarían adoptar los Principios sugeridos para alcanzar una Aproximación Basada en Resultados?

10. ¿Cómo se pueden mejorar los Principios sugeridos?

Regular en Busca de Resultados– Estrategias y Prioridades para promover el Liderazgo y la construcción de relaciones efectivas

Introducción & Resumen

El ecosistema regulatorio sobre datos personales y privacidad está cambiando rápidamente, y no sólo dentro de la UE. Durante muchos años, CIPL ha promovido el rol de las organizaciones responsables (*accountable*) y las bondades de una aproximación basada en riesgos. Ahora queremos explorar el "andamiaje" del sistema como un todo y considerar cómo hacer que sus componentes individuales encajen mejor.

El propósito de este artículo en particular es estimular las discusiones sobre cómo las Autoridades de Protección de Datos[1] (APDs) pueden maximizar su efectividad en la era moderna de la información.

Cuando las funciones son numerosas, las expectativas son altas y los recursos son limitados. En este escrito se pone de presente la pregunta sobre la conveniencia de dedicar esfuerzos, y cómo hacerlo, para que la vigilancia[2] de datos personales se "oriente más a obtener resultados". Esto implica tomar decisiones difíciles, pero esenciales, sobre estrategias y prioridades. Las APDs, sencillamente, no pueden hacerlo todo.

La Aproximación Basada en Resultados ha venido siendo usada por CIPL para significar la manera en que las APDs –de forma independiente y colaborativa- pueden maximizar su efectividad mediante la adopción de aproximaciones modernas y estratégicas a la supervisión de forma tal que les permita alcanzar los mejores resultados para los individuos, la sociedad y las organizaciones vigiladas. De manera concreta, implica relacionarse de manera responsable y colaborativa con aquellas organizaciones, tanto en el sector público como en el privado, que están tratando de "hacer lo correcto", como con aquellas que no.

Este artículo sugiere algunos principios de alto nivel que pueden servir como base para una Aproximación Basada en Resultados. Los principios han sido pensados como una herramienta para la definición de prioridades estratégicas, incluyendo el desarrollo de rankings de los diferentes tipos de funciones, la selección de las herramientas más apropiadas y la forma para dirigir esfuerzos a algunos sectores, actividades u organizaciones.

[1] "Autoridades de Protección de Datos", tal y como se usa en este artículo, equivale a aquellas con membrecía en la Conferencia Internacional de Comisionados de Protección de Datos y Privacidad.
2 Nota de la traducción: En este artículo se usan los términos regulación, vigilancia y supervisión pare referirse a las actividades de las Autoridades de Protección de Datos en ejercicio de sus funciones.

Principios para una Aproximación Basada en Resultados

- Para poder Vigilar en busca de Resultados en un mundo digital, se requieren Autoridades de Protección de Datos independientes y que sean estratégicas, efectivas, coordinadas y transparentes.

- El objetivo de una APD debe ser producir resultados efectivos en términos de costos, que protejan realmente a los individuos, promuevan usos responsables de la información y faciliten la prosperidad y la innovación

- Las APDs deben tener la protección de los individuos en lo más alto de sus prioridades.

- Cada APD independiente debe ser responsable de informar sobre los resultados que busca alcanzar y las prioridades y aproximaciones que adoptará para alcanzar esos resultados en su labor de vigilancia.

- Las estrategias de todas las APDs deben ser tan coordinadas, consistentes y complementarias como sea posible.

- Cada APD debe adoptar una aproximación basada en riesgos para todas sus actividades, fijando las prioridades en aquellas conductas que generen mayor riesgo a los individuos o a los valores democráticos y sociales.

- Una aproximación basada en el relacionamiento constructivo con énfasis en liderazgo, información, asesoría, diálogo y apoyo será más efectiva que la simple y excesiva dependencia en la disuasión y el castigo.

- El énfasis en la información y la asesoría es especialmente importante en el área de protección de datos, debido a su amplio impacto en tantas organizaciones y a la naturaleza de los requerimientos que, o son imprecisos, o son determinados por el contexto, requiriéndose que haya juicios de valor caso por caso.

- Las relaciones abiertas y constructivas con las organizaciones que tratan datos personales, basadas en un diálogo constructivo y en la cooperación mutua, pero sin caer en responsabilidades difuminadas, mejorarán los resultados generales de cumplimiento legal.

- Las organizaciones vigiladas deben ser evaluadas particularmente con referencia a la buena fe demostrable y a la debida diligencia empleada en sus esfuerzos para cumplir con la ley.

- Las organizaciones que intentan comportarse de manera responsable para "hacer lo correcto" deben tener incentivos para identificarse, por ejemplo mediante la demostración transparente de su responsabilidad proactiva, sus programas de protección de datos y gestión de riesgos, la influencia de sus Oficiales de Protección de Datos (OPDs) y el uso de sellos y programas de certificación, BCRs, CBPR y otros marcos de responsabilidad proactiva

(*accountability)*.

- Las sanciones punitivas deben dirigirse principalmente a la actividad que, de manera consciente, deliberada, seriamente negligente, reiterada o particularmente grave, incumpla con la ley.

- Las APDs deben tratar a las organizaciones vigiladas de manera consistente—adoptando aproximaciones similares dentro de ciertos sectores, independientemente del tipo o alcance geográfico de la organización.

- Aunque la necesidad de gestionar quejas individuales puede ser un componente importante para proteger a los individuos, manejar volúmenes muy altos consume muchos recursos y puede impedir alcanzar metas estratégicas más amplias. Las quejas deben ser gestionadas con criterios estrictos y claros para determinar el alcance de las investigaciones, y también teniendo en cuenta que son un recurso de inteligencia muy valioso.

El objetivo principal de este artículo es estimular la discusión dentro de la comunidad de protección de datos y privacidad (incluyendo autoridades, organizaciones vigiladas, sociedad civil, académicos y expertos).

Aun cuando este artículo apunta a ofrecer una aproximación a cómo podría verse en la práctica esta aproximación a la protección de datos basada en resultados, será en últimas una decisión de la comunidad de APDs optar por desarrollar con mayor detalle esta propuesta y cómo hacerlo. Si la esencia de estos Principios logra un consenso amplio, se prevé que podría adoptarse, promulgarse y ponerse en práctica una versión revisada en cuatro niveles:

- Globalmente, por la Conferencia Internacional de Comisionados de Protección de Datos y Privacidad (ICDPPC)[3]. Un objetivo razonable sería apuntarle a la 40 Conferencia Internacional, que se llevará a cabo en Bruselas en octubre de 2018.
- A nivel de la UE, por la Comité Europeo de Protección de Datos.
- A nivel de Asia – Pacífico por el foro de Autoridades Asia Pacífico (APPA).
- A nivel operativo, por el Global Privacy Enforcement Network (GPEN) y el APEC Cross-border Privacy Enforcement Arrangement (CPEA)[4].

Estructura de este Artículo

La Sección 1 elabora sobre el propósito y la naturaleza de este artículo, haciendo énfasis en la necesidad de una aproximación estratégica para establecer prioridades

[3] www.icdppc.org.
[4] El CPEA, disponible en http://www.apec.org/~/media/Files/Groups/ECSG/CBPR/CBPR-CrossBorderPrivacyEnforcement.pdf, es un MOU de cooperación en investigaciones para las autoridades de protección de datos de APEC. Prevé, entre otras cosas, que las autoridades participantes pueden priorizar sus acciones investigativas, tanto individual como colectivamente. *Ver* CPEA en la Sección 9.2.

que aseguren la consecución de los mejores resultados. En la sección se ponen de presente los beneficios potenciales para los individuos, las APDs y los vigilados. El artículo tiene como objetivo ser útil para todas las APDs a nivel global, alentando además que se alcance la máxima consistencia para una economía global digital. Hay un énfasis marcado en la Unión Europea donde el RGPD traerá consigo cambios significativos en la manera en que las APDs europeas trabajan tanto individual como conjuntamente.

La Sección 2 examina las múltiples funciones que se han encargado a las APDs con una particular referencia a aquellas prescritas por el RGPD. Desde mayo de 2018 esto les dará a las APDs a lo largo de Europa un rol sin precedentes. El RGPD contempla alrededor de 22 "tareas" separadas y 27 poderes separados, pero sin un sentido de misión estratégica. Para ayudar en las dinámicas de priorización, las funciones se han agrupado por referencia a cuatro tipos:

1. **"Líder"** – las funciones que se basan en la experticia, la autoridad y el apoyo de la APD;
2. **"Oficial de Policía"** – donde se contemplan medidas investigativas y sancionatorias por violación de normas, especialmente aquellas violaciones culposas o deliberadas;
3. **"Gestor de Quejas"** – donde las quejas pueden llevar directa o indirectamente a una sanción o a un mecanismo de compensación;
4. **"Autorizador"** – donde se requiere algún tipo de autorización previa por parte de la APD.

La Sección 3 ilustra la escasez de recursos disponibles para las APDs. Tomando a la UE como ejemplo, unas 26 millones de empresas caen dentro de la jurisdicción de sus APDs. Las últimas estadísticas muestran que los presupuestos para las APDs en 26 países de la UE promediaron menos de €0.41 por ciudadano y más o menos €8 por negocio. Otro estudio muestra que solo 9 de 19 APDs tenían más de 40 funcionarios de tiempo completo y seis tenían menos de 30 empleados. La sección concluye con un llamado a incrementar los presupuestos de las APDs, sugiriendo que simplemente mediante el cobro de una tasa anual de tan solo €20 a cada organización vigilada en la UE, podrían recogerse por lo menos €500 millones para las APDs de la UE.

La Sección 4 se refiere a la evidencia sobre regulación y vigilancia efectiva en otras esferas regulatorias. Aquí se ha tomado mucha información de una serie de estudios recientes, particularmente del trabajo del Profesor Christopher Hodges en *Law and Corporate Behaviour* (Derecho y Comportamiento Corporativo[5]) que es un sondeo completo sobre las aproximaciones modernas a la regulación, las medidas de cumplimiento de la ley (*enforcement*), el cumplimiento legal (*compliance*) y la ética. Hace énfasis en el resultado óptimo de cualquier Sistema de Vigilancia para

[5] https://www.bloomsbury.com/in/law-and-corporate-behaviour-9781782255826/.

producir comportamientos aceptables y para detener los inaceptables. En términos prácticos, una vigilancia efectiva implica asegurar el máximo nivel de cumplimiento. La mayoría de las organizaciones buscan “hacer lo correcto” mediante el cumplimiento de sus responsabilidades. Esto significa que, si las autoridades son serias sobre su objetivo de ser efectivas, deben priorizar sus funciones de apoyo, construyendo relaciones abiertas y constructivas entre las autoridades y sus vigilados. La disuasión y el castigo tienen una efectividad limitada y deben dirigirse principalmente contra aquellos que de forma consciente y deliberada están violando la ley.

La Sección 5 es la médula de este artículo de discusión, y busca la aplicación de estas lecciones a la supervisión y vigilancia en privacidad y datos personales. Allí se discute qué debe entenderse por efectividad y resultados. Sugiere que, para ir más allá del mero cumplimiento legal con requerimientos formales, la vigilancia en datos personales debe apuntar hacia un mundo digital donde las personas se desarrollen con dignidad como individuos autónomos. Los resultados generales que se buscan podrían entonces desarrollarse a lo largo de las siguientes líneas:

- La prevención de los usos de datos que menoscaben la calidad de vida de los individuos negándoles su derecho a la privacidad y la protección de datos; y
- La promoción de una sociedad donde una buena calidad de vida para sus miembros fluya de una genuina y extendida protección de datos donde el uso de la información en un mundo digital sea tanto universal como popular.

La sección aborda, en el contexto de las funciones crecientes y los recursos escasos, la necesidad de contar con prioridades estratégicas para las APD que ayuden a alcanzar estos objetivos. Aunque hay algunas categorías cruzadas, los cuatro tipos principales de funciones se agrupan juntas y se relacionan con los cuatro objetivos regulatorios principales: **Predecir – Prevenir - Detectar - Sancionar**. El concepto de una Aproximación Basada en Resultados para Protección de Datos se desarrolla a partir de este análisis y de la evidencia de otras esferas regulatorias. En particular, se sugiere que el rol de **Liderazgo**, con un componente de diálogo y **Relacionamiento Constructivo** con las organizaciones vigiladas, debe ser la prioridad más alta.

La Sección 6 elabora sobre lo que significa Relacionamiento Constructivo en la práctica y da ejemplos de las actividades y técnicas que probablemente permitirán que se alcancen mejores resultados. Se hace énfasis en la transparencia, los mecanismos de consulta, los intercambios sinceros y el aprovechamiento de la tendencia de las organizaciones de seguir al líder de la manada (“efecto rebaño”) así como la presión competitiva y de grupo.

La Sección 7 establece un primer borrador para una Aproximación Basada en Resultados y sugiere cómo (después de un debate y una revisión completa) puede adoptarse y promulgarse.

La Sección 8 aborda los posibles problemas con la aproximación sugerida. Da respuestas a las preocupaciones sobre las consecuencias de tener que tratar algunas funciones como prioridad baja, los riesgos de la “captura regulatoria” y el riesgo de que algunos vigilados pueden temer un acercamiento muy cercano con las autoridades.

Preguntas para Discusión

Este es un artículo de discusión. En esa medida, las preguntas clave se hacen al final de la sección pertinente. CIPL prevé que, a su debido tiempo, enviará estas preguntas en cartas abiertas a los líderes de la Conferencia Internacional, el Grupo de Trabajo del Artículo 29 (GT29) / CEPD, el foro APPA, GPEN y el CPEA. Por motivos de conveniencia, las Diez Preguntas de Discusión se presentan juntas en la página 4 anterior.

Agradecimientos

Este artículo de discusión se ha desarrollado como un proceso dinámico y las preguntas planteadas implican que se requieren muchas respuestas. Muchas personas, incluyendo muchas que actualmente o en el pasado formaron parte de una APD, han hecho aportes que han mejorado de manera significativa este artículo. Mención especial merece la Secretaría de la Conferencia Internacional de Comisionados de Protección de Datos y Privacidad por haber puesto a disposición los datos de su reciente censo de APDs.

Las APD, la industria y los académicos que participaron en el taller que CIPL organizó en Dublín en junio de 2017 para revisar el borrador de este artículo, estuvieron de acuerdo en la importancia del tema e hicieron contribuciones valiosísimas, particularmente relacionadas con articular la forma en que el “Relacionamiento Constructivo” operaría en la práctica.

CIPL está inmensamente agradecido con todos los participantes que de manera entusiasta han ayudado en este Proyecto.

1. Propósito y naturaleza de este artículo

La protección de datos se encuentra en un momento crucial. Con la cuarta revolución industrial[6] y las prácticas de información cambiando de manera vertiginosa, así como con la nueva generación de leyes y regulaciones de protección de datos, incluyendo el RGPD europeo, las apuestas nunca habían sido tan elevadas.

Cada Autoridad de Protección de Datos independiente (APD) juega un papel crucial en lograr que la protección de datos sea una realidad. Sin embargo, en algunas ocasiones, el rol general de las APDs y sus funciones específicas se dan por descontadas sin mucho análisis detallado sobre cómo deben ejercerse en la práctica.

El objetivo de este artículo de discusión es formular preguntas sobre cómo puede maximizarse —de cara a los múltiples retos y a las altas expectativas- la efectividad de un marco regulatorio. Este objetivo se logra mediante la búsqueda de respuestas a una Aproximación Basada en Resultados en línea con los desarrollos que se han alcanzado en otras esferas regulatorias. Esto implica adoptar una aproximación estratégica para alcanzar prioridades y así alcanzar los mejores resultados.

El significado completo y la naturaleza de una Aproximación Basada en Resultados se elaboran a continuación. Pero primero resulta de gran ayuda definir los beneficios que se busca identificar mediante esta discusión. Estos se pueden agrupar de la siguiente forma:

a. Beneficios para los individuos

El objetivo básico de la regulación de protección de datos debe ser proteger a los individuos al tiempo que se facilitan los flujos libres de información[7]. La regulación de protección de datos promueve la confianza, elemento que es esencial para el progreso y el crecimiento digital, la innovación y el uso beneficioso de los datos.

La aproximación de la UE, y la de muchas otras jurisdicciones, expresa esto en términos de proteger los derechos y las libertades fundamentales. En otras partes, el propósito se ve más en términos de prevenir el daño a los individuos. En todos los casos, hay también un contexto más amplio de “bienestar social”. Cualquiera que sea el lenguaje utilizado, cualquier marco regulatorio debe dar una alta prioridad a asegurar la protección de las personas.

[6] En los términos en que lo ha entendido el Foro Económico Mundial.
[7] La Corte Europea de Justicia ha exigido que las APDs establezcan un “balance justo entre la protección del derecho a la vida privada y el libre movimiento de datos personales”. (Caso C-518/07 – par. 30).

Cualquier marco regulatorio debe ser efectivo y la efectividad debe ser principalmente medida en términos de impacto a los individuos. ¿Están siendo protegidos en la práctica y no sólo en el papel? ¿Están recibiendo los beneficios a los que tienen derecho? ¿Las personas (consumidores, ciudadanos, empleados) son capaces de maximizar las ventajas de la sociedad digital con la confianza de que sus intereses están siendo debidamente protegidos? ¿Pueden esperar que las organizaciones realmente van a gestionar la información personal de forma correcta?

También se deben hacer balances en términos de sensibilidades frente a las necesidades y los intereses de los individuos cuando están lidiando con entidades comerciales y públicas. Las personas normalmente no tienen el poder, el conocimiento o la capacidad de salvaguardar enteramente sus intereses por su propia cuenta. Pero las características, actitudes y preferencias de los individuos varían considerablemente, y la presunción debe ser que ellos son los mejores jueces de sus propios intereses. De la misma forma, el mercado y la presión de los competidores pueden tener un impacto significativo sobre la reputación y los comportamientos organizacionales. Cualquier cuerpo regulatorio debe tener mucho cuidado para evitar sugerir que "sabe lo que es más conveniente" cuando se trata de decidir sobre aquello que es mejor para la gente. Una aproximación moderna le da precedencia a proteger y empoderar a los individuos, sin subestimarlos ni restarles autonomía[8].

Un enfoque basado en las personas también es vital para comunicar los mensajes a los medios en lenguaje sencillo con el objetivo explícito de promover la conciencia del público y generar apoyo popular para las actividades de protección de datos[9]. A menos de que los individuos entiendan la importancia de la protección de datos, y puedan relacionarla con sus propias vidas, esta nunca será plenamente efectiva.

b. Beneficios para las APDs

Las APDs enfrentan muchos retos. Se han convertido en los principales reguladores de la sociedad digital y de la información que la hace funcionar. Se espera de ellas que ejerzan control sobre millones de organizaciones—grandes, medianas y pequeñas, que operan en los sectores público y privado y muchas veces a través de las fronteras nacionales. La tecnología innovadora se desarrolla a diario. Los individuos opinan cada vez más sobre sus expectativas de privacidad y los usos responsables de datos. Las APDs deben balancear numerosas tareas y objetivos de política pública potencialmente en competencia —protección de datos, otros derechos fundamentales (incluyendo la libertad de

[8] La estrategia del SEPD contiene un muy bienvenido compromiso de comunicar incluso los conceptos difíciles en lenguaje sencillo y claro.
[9] Tal y como se pone de manera explícita en el artículo 57(1)(b) del RGPD.

expresión), los flujos libres de información, innovación, beneficios sociales, seguridad, entre otros.

Aún más, en términos absolutos y en comparación con otras áreas regulatorias, las APDs están tremendamente desfinanciadas. Un reto fundamental para cualquier APD es cómo maximizar la efectividad cuando hay tantas cosas que podrían hacer y tan pocos recursos para hacerlo. Los recursos pueden incrementarse para situaciones individuales, pero no es una afirmación controversial afirmar que los recursos nunca serán adecuados. Las APDs también deben mantener su credibilidad y legitimidad. Las APDs nunca estarán en capacidad de hacerlo todo.

La búsqueda es entonces hacia aproximaciones que incrementen la efectividad y la influencia de las APDs y que hagan el mejor uso posible de los recursos disponibles concentrándose en aquellas actividades de vigilancia que prometen los mejores resultados. Puesto de otra forma, la credibilidad e inclusive la legitimidad de las APDs pueden ser cuestionadas si no toman medidas activas. para maximizar la efectividad.

La necesidad de tener aproximaciones consistentes se vuelve aun mayor con las demandas de cooperación y colaboración transfronteriza. La globalización de los flujos de información, y la necesidad de proteger los derechos de los individuos globalmente, debe implicar igualmente un esfuerzo de armonizar las funciones y los poderes de las APDs. Dentro de la UE, esto se contempla en el RGPD.

Para que cualquiera de estas aspiraciones funcione efectivamente, debe haber total claridad sobre las estrategias y prioridades de todas las autoridades participantes. Una Aproximación Basada en Resultados no significa una aproximación estandarizada para todos. Pero sí significa por lo menos que la comunidad internacional de APDs tenga confianza en que actuarán en formas que sean complementarias y convergentes. Aun cuando las APDs operan en diferentes sistemas legales y son parte de distintas culturas regulatorias, es esencial en un mundo digital sin fronteras que las prioridades de las APDs sean mutuamente consistentes y tan fluidas como sea posible. Esto también mejorará el uso eficiente de los recursos de las APDs.

Dentro de la UE, estas necesidades son aún más evidentes. El mecanismo de cooperación y consistencia introducido por el RGPD necesitará tanto consistencia en los enfoques de prioridades y medidas para hacer cumplir la ley como consistencia en materia de interpretación legislativa.

La cooperación internacional ya ha mostrado su potencial con iniciativas tales como el Global Privacy Enforcement Network (GPEN) y el APEC Cross-border Privacy Enforcement Arrangement (CPEA), con

investigaciones coordinadas y un Barrido Internacional de Internet.

También ha habido esfuerzos crecientes para cooperar con las autoridades de protección al consumidor, competencia, telecomunicaciones y otros. El EDPS ha propuesto el establecimiento de una Biblioteca Digital para "acercar a las agencias de las áreas de competencia, consumidor y protección de datos que estén dispuestas a compartir información y discutir cómo hacer cumplir la ley teniendo en mente el interés de los individuos". La primera reunión de la "Biblioteca" se llevó a cabo en mayo de 2017.[10]

c. Beneficios para los vigilados

Todas las organizaciones—compañías grandes y pequeñas, gobiernos, entidades públicas, ONGs—están digitalizando sus actividades, productos y servicios, tratando datos personales y sujetas en mayor o menor medida a leyes de protección de datos personales. Por su naturaleza, las leyes no pueden ser claramente prescriptivas y en muchas ocasiones están basadas en principios y en el contexto aplicable. Ello no obstante, los vigilados deben saber cómo comportarse, qué acciones se esperan de ellos para proteger a los individuos y qué comportamientos deben evitar. Todos los vigilados, organizaciones grandes, PYMES y emprendimientos, necesitan y tienen igual derecho a tanta consistencia y predictibilidad como sea posible de los cuerpos regulatorios dentro y fuera de las fronteras nacionales. Esto es especialmente importante dada la creciente velocidad de los desarrollos tecnológicos y el hecho de que las leyes de protección de datos modernas le dan un peso cada vez mayor a la responsabilidad demostrada (*accountability*) y la gestión de riesgos.

Un marco regulatorio efectivo para la economía digital, con flujos de información fáciles y libres, pero bien ordenados, es esencial para promover la innovación, el crecimiento económico y la prosperidad. El marco no debería, sin embargo, imponer cargas desproporcionadas, especialmente allí donde los costos se conviertan en incrementos de precios, menores salarios o impuestos más altos.

d. El mundo en general, Europa en específico

Las APDs alrededor del mundo tienen mucho más en común que aquellas diferencias específicas que pueden diferenciarlas. El análisis y las sugerencias de este artículo están entonces pensadas para ayudarles a todas las APDs, además de promover la máxima consistencia para la economía digital global.

[10] https://edps.europa.UE/data-protection/our-work/subjects/big-data-digital-clearinghouse_en.

Al mismo tiempo, las actividades de las APDs en la UE serán transformadas muy pronto por el RGPD. Esto tendrá implicaciones enormes para ellas, pero también para muchas otras APDs que estarán directa o indirectamente afectadas por el RGPD. El rebarajamiento de las funciones de las APD—y en particular la ventanilla única (*one-stop-shop*) con una APD principal, así como la cooperación obligatoria y los mecanismos de consistencia—cristalizan la necesidad para un elevado consenso sobre cómo maximizar la efectividad. Todas las APDs en la UE tendrán que repensar sus prioridades estratégicas y hacerlo de forma consistente a lo largo de la UE. Mientras se adoptan las medidas que les permitan estar a la altura de estos retos, CIPL espera que los análisis y las sugerencias que se plantean en este artículo sean especialmente útiles para dichas APDs, para el GT 29 y (a su debido tiempo) para el CEPD.

Es de esperarse que la aproximación de la UE en los próximos años tenga un efecto significativo en el resto del mundo. Aunque este artículo se basa principalmente en el RGPD para ilustrar muchas de sus secciones, y anticipa que el CEPD podría jugar un papel de liderazgo en llevar hacia adelante dichas sugerencias, también se debe enfatizar que la aproximación general no está pensada para que se limite al contexto europeo.

2. Las funciones de las Autoridades de Protección de Datos

Aunque los detalles de las funciones específicas de las APDs varían alrededor del mundo, hay algunas semejanzas generales. En 2001, la Conferencia Internacional de Comisionados de Protección de Datos y Privacidad adoptó los criterios para reconocer las credenciales de las autoridades de protección de datos[11].

Mucho peso se le ha dado a la genuina independencia y autonomía de las APDs. Pueden ser independientes y autónomas, pero necesitan ejercer sus funciones con un criterio de interés público. En 2010 el caso de la *Comisión v. Alemania*[12] el Tribunal de Justicia de la Unión Europea enfatizó cómo las APDs encajan dentro del sistema de pesos y contrapesos en una democracia basada en el Estado de Derecho.

Las APDs pueden ser vistas como cuerpos "híbridos", de los que se espera que las organizaciones cumplan con sus obligaciones, que los sujetos de los individuos se respeten y (de forma más general) que se alcancen altos niveles de privacidad y protección de datos a través de toda la sociedad. Su meta estratégica puede ser descrita en términos de balancear la protección de los derechos fundamentales—o la prevención del daño—con el flujo libre de datos y los usos benéficos de la información. En la UE, la Corte Europea de Justicia describió la esencia de la tarea de la APD como "el establecimiento de un balance justo entre la protección del derecho a la vida privada y el libre movimiento de datos personales"[13]. Las APDs han sido descritas como "promotores de la autoridad"[14].

En la UE, las APDs tienen un estatus constitucional con la misión amplia de "vigilar" o "supervisar" el tratamiento de datos personales y asegurar el cumplimiento con las normas de protección de datos[15]. Los artículos 57 y 58 del RGPD establecen algunas de las funciones—algunas de ellas nuevas—de cada autoridad de protección de datos. Estas pueden ser vistas como una mezcla de "zanahoria y garrote". Se dividen en tareas y poderes. Se identifican 22 "tareas" separadas, donde la APD "debe" llevar a cabo la actividad prescrita. Estas se amplían con 27 poderes, de los cuales 6 son "investigativos", 11 son "correctivos" y 10 (con algunas réplicas de las tareas obligatorias) son de "autorización" y "consulta".

En efecto, el RGPD contiene 22 tareas obligatorias y 27 poderes a manera de lista de mercado y con poco o ningún intento de priorizar o indicar cómo se relacionan entre sí, ni ninguna articulación sobre la misión general de cada APD en términos de los resultados que se supone deben alcanzar. Cada función es fácil de explicar

[11] https://icdppc.org/wp-content/uploads/2015/02/Criteria-and-Rules-for-Credentials-Committee-and-the-Accreditation-Principios.pdf.
[12] C-518/07 - para 41-43.
[13] C-518/07 - para 30.
[14] Bennett y Raab, *The Governance of Privacy*.
[15] Artículo 16(2) del Tratado de la Unión Europea y Artículo 8(3) de la Carta de Derechos Fundamentales.

aisladamente, y la mayoría no son ni controversiales ni sorprendentes en sí mismas. Sin embargo, y esto es crítico, el RGPD no plantea en ningún sentido una estrategia general.

Ello no obstante, nada en el RGPD, o en otras leyes a nivel mundial, va en contra del desarrollo de una aproximación más estratégica y basada en resultados. También es posible identificar los diferentes **tipos** de funciones—un elemento esencial para cualquier pensamiento estratégico.

Aunque hay vínculos e interdependencias, sin fronteras rígidas, el Anexo A de este artículo de discusión agrupa cada una de las funciones del RGPD en uno de cuatro tipos principales y generales:

1. **"Líder"** – las funciones que se basan en la experticia, la autoridad y el apoyo de la APD;
2. **"Oficial de Policía"** – donde se contemplan medidas sancionatorias por violación de normas, especialmente aquellas violaciones culposas o deliberadas;
3. **"Gestor de Quejas"** – donde las quejas pueden llevar directa o indirectamente a una sanción o a un mecanismo de compensación;
4. **"Autorizador"** – donde se requiere algún tipo de autorización previa por parte de la APD.

3. Recursos Escasos de las APD

Aunque sean adecuados, deben discutirse los recursos disponibles para las APDs antes de explorar las estrategias y prioridades para maximizar la efectividad de la regulación.

a. Nivel de recursos

El más reciente sondeo comparativo de los presupuestos de las APDs se adelantó como un censo por la ICDPPC en 2017.[16] Alguna información relevante del sondeo se incluye y analiza con más detalle en el Anexo B y se compara con algunas de las cargas que tienen las APDs[17].

Las respuestas del sondeo incluyen información sobre recursos para 87 APDs de 58 países. De aquellos países que entregaron información financiera, el presupuesto total global para las APDs para 2016 fue de €887,320,351.

Para 26 países de la UE[18] las cifras muestran un presupuesto total en 2016 de €205,703,574 para una población total ese año de 507,471,970.[19] Esto sugeriría, en este grupo de 26 países tomados en conjunto, que el presupuesto por ciudadano es de menos de €0.41.

Aún más diciente de la carga que se impone a cada APD es la necesidad de relacionar los recursos con el número de organizaciones vigiladas. Eurostat estima que "en 2014, la economía de los negocios del grupo EU 28 estaba conformada por alrededor de 26 millones de empresas activas"[20]. Asumiendo que virtualmente todas las organizaciones hacen hoy en día tratamiento de datos, esto sugiere que las APDs tienen un presupuesto promedio de solo alrededor de €8 por organización.

Los números de personal dan una indicación adicional de los recursos y las capacidades. El reciente estudio de PHAEDRA titulado *Enforcing Privacy*[21] *("Haciendo cumplir la Privacidad")* encontró que sólo 12 APDs en la Unión Europea tenían más de 40 personas de tiempo completo en 2015, la más alta con 350 y las más pequeñas con 14. Seis de las APDs de la UE tenían un personal inferior a 30 personas.

---

[16] La información está disponible por solicitud en la Secretaría de la Conferencia Internacional de Comisionados de Protección de Datos y Privacidad, https://icdppc.org/the-conference-and-executive-committee/icdppc-census/.

[17] CIPL está muy agradecido con ICDPPC por poner a disposición la información del sondeo para usarse en este artículo antes de su publicación oficial.

[18] Las cifras no estaban disponibles para Austria ni Croacia y la cifra para Alemania es menor que el valor actual dado que solo 7 de 16 Länder entregaron datos.

[19] Las cifras de población para los 26 países relevantes de la UE se obtuvieron del Banco Mundial el 27 de julio de 2017, http://data.worldbank.org/indicator/SP.POP.TOTL.

[20] http://ec.europa.UE/eurostat/statistics-explained/index.php/Business_demography_statistics.

[21] http://www.phaedra-project.UE/wp-content/uploads/phaedra1_enforcing_privacy_final.pdf.

La escasez de los recursos no es nueva y es reconocida por las propias APDs. Un reciente reconocimiento colectivo del problema se encuentra en una Resolución[22] adoptada en la Conferencia de Autoridades Europeas de Protección de Datos en mayo de 2015. Los extractos del preámbulo y la sustancia de la Resolución ameritan su cita en este documento:

- "…las Autoridades Europeas de Protección de Datos están confrontando muchos retos nuevos, con implicaciones en la manera como llevan a cabo sus funciones …".
- "…las Autoridades de Protección de Datos de manera incremental están encontrándose con problemas de financiación y otras limitaciones de recursos al mismo tiempo en que incrementan sus funciones".
- "…los derechos y las obligaciones sobre el papel siempre deben hacerse cumplir y ser realizables o corren el riesgo de convertirse en una ilusión, o aun peor, en una desilusión para los ciudadanos".
- "[La Conferencia] hace un llamado a los gobiernos de los países europeos para que garanticen que el financiamiento de las Autoridades de Protección de Datos sea suficiente para alcanzar las demandas crecientes que se les vienen imponiendo y para asegurar que los requerimientos fijados por los legisladores se puedan aplicar en la práctica".

A pesar de la magnitud de las responsabilidades que el RGPD deposita sobre las APDs, estehace pocos esfuerzos para incrementar los de por sí muy limitados recursos financieros y humanos con que cuentan. El Artículo 52(4) establece solo en términos generales que *"(c)ada Estado miembro garantizará que cada autoridad de control disponga en todo momento de los recursos humanos, técnicos y financieros, así como de los locales y las infraestructuras necesarias para el cumplimiento efectivo de sus funciones y el ejercicio de sus poderes (…)".*

Esto es, sin embargo, poco más que una exhortación general con más aspiraciones que precisiones u obligaciones reales. No es específica y será difícil hacerla cumplir por medios legales, políticos o de otra naturaleza[23]. La Comisión Europea está presionando a los Estados Miembros para que provean financiación adecuada, pero no ha desarrollado ningún criterio para evaluar qué es adecuado o 'necesario'".

Existe alguna evidencia de incrementos actuales y potenciales. El presupuesto de la Comisión Irlandesa de Protección de Datos ha sido aumentado sustancialmente—el censo de la ICDPPC reporta un incremento de más de 20 % sólo para el periodo 2015-16. En Holanda, la Autoriteit Persoonsgegevens (AP) comisionó una serie de consultorías para revisar qué recursos necesitará para asumir sus responsabilidades bajo el RGPD. El reporte de la consultoría[24] concluyó que la

[22] https://edps.europa.UE/sites/edp/files/publication/15-05-20_manchester_resolution_1_en_0.pdf.
[23] En el caso de la *Comisión v. Austria* el TJUE ni siquiera adoptó el argumento de que una APD debería tener su propio presupuesto separado.
[24] https://www.tweedekamer.nl/kamerstukken/detail?id=2017D15344&did=2017D15344.

nueva situación sería completamente diferente. Enfatizó los volúmenes incrementales de quejas y reportes de incidentes de seguridad, la necesidad de mayores controles sistémicos y más investigaciones derivadas de los mecanismos de cooperación de la UE, los costos de promover la concientización pública y organizacional, la necesidad de adelantar consultas previas en las Evaluaciones de Impacto de Protección de Datos (EIPD) y los costos asociados a los acuerdos de certificación y acreditación. De conformidad con este nuevo escenario, esta nueva realidad podría implicar un aumento de la planta de personal de 72 a 185-270 personas. El reporte se encuentra actualmente en el Ministerio de Seguridad y Justicia, donde se espera la adopción de decisiones presupuestales.

Las indicaciones de incrementos actuales o potenciales en Irlanda, Holanda y otros países son bienvenidas. No obstante, el panorama general no parece extenderse más allá de incrementos puntuales por lo cual se mantiene como una preocupación importante.

Finalmente, no se ha puesto suficiente atención a la necesidad de las APDs de contratar más expertos en tecnología, comunicaciones y otras disciplinas para ir más allá de los conocimientos legales que se encuentran en la gran mayoría de APDs.

b. ¿Recursos adicionales?

Sin duda, cualquiera que sea la aproximación adoptada por las APDs europeas, necesitarán recursos adicionales. El estudio de PHAEDRA[25] concluyó que “hoy en día– para asegurar un nivel adecuado de protección de la privacidad y los datos personales y para investigar y perseguir las violaciones que se presenten– estas autoridades de supervisión se encuentran con limitaciones en forma de falta de recursos humanos o presupuestales…”. El estudio cita la visión de la Agencia de los Derechos Fundamentales de la Unión Europea en 2014 en el sentido de que “el problema de los recursos representa uno de los grandes obstáculos que limitan su actividad”.

Los recursos están muy alejados de aquellos disponibles para las autoridades de competencia. Un reciente, aunque no completo, estudio adelantado por *Politico* concluyó que “unos hambrientos perros guardianes están colgados en su preparación para la más grande ley de protección de datos de la UE”[26]. En marzo de 2017, Isabelle Falque-Pierrotin en nombre del GT29 envió una carta[27] al Consejo de Ministros pidiendo el incremento de los presupuestos para permitirles a las APDs

---

[25] En la página 16.
[26] http://www.politico.UE/pro/starving-watchdogs-will-police-UE-biggest-privacy-law-general-data-protection-regulation-europe/?utm_source=POLITICO.UE&utm_campaign=edc4d71000-EMAIL_CAMPAIGN_2017_04_04&utm_medium=email&utm_term=0_10959edeb5-edc4d71000-189890157.
[27] http://ec.europa.UE/newsroom/document.cfm?doc_id=43668.

“llevar a cabo de manera efectiva sus nuevas tareas, entrenar a su propio personal, mejorar sus sistemas de TI, promover la concientización y preparar guías sobre las nuevas reglas”.

El RGPD no hace referencia a las posibles fuentes para el financiamiento de las APDs, sino que le deja esta tarea a los Estados Miembros. Hay fundamentalmente tres posibles fuentes:

- **Fondos gubernamentales**– Los recursos públicos, obtenidos del cobro de impuestos o de fuentes de financiamiento, han sido un recurso tradicional de presupuesto para la mayoría de las APDs. Pero, con muchos gobiernos enfrentando retos en una “era de austeridad”, uno debe preguntarse qué tan realista es, o qué tan probable, que los gobiernos nacionales provean incrementos significativos obtenidos de fondos públicos adicionales a los ya disponibles para las APDs. Igualmente, allí donde los presupuestos dependen de la financiación del estado, y especialmente cuando no hay garantías constitucionales para un adecuado financiamiento, existe una posibilidad real de pérdida de independencia.

- **Multas**– El RGPD contempla multas sustanciales para las organizaciones que violan sus obligaciones. Pero cualquier intento de financiar a las APDs directamente de las multas que ellas mismas imponen, será fieramente atacada como una práctica de incentivos perversos. Cualquier intento en ese sentido estará sujeta a cuestionamientos éticos, políticos y legales.

- **Vigilados** – El costo de la vigilancia podría ser directamente asumido por los sujetos vigilados, ya sea mediante el pago de tasas o por otros mecanismos. Este enfoque de “*el que contamina paga*” es cada vez más usado en otras áreas. Algunas APDs recibirían ingresos por servicios que se pueden cobrar, tales como auditorías, entrenamientos y publicaciones. La aproximación reconoce que la regulación beneficia a las organizaciones mediante el incremento en la confianza del público y en sus actividades, además de que evita imponer una carga elevada a los recursos públicos. También puede ser muy sencillo en términos administrativos y barato de cobrar. El RGPD no prevendría, por ejemplo, que un Estado Miembro introdujera un requisito básico para que cada organización que trata datos personales pague una módica tasa anual en línea, directa o indirectamente, a cada APD.

Asumiendo una vez más que virtualmente todas las empresas hoy en día están tratando datos personales, una tasa nominal de sólo €20 a las 26 millones de empresas que hay en la UE generaría un presupuesto total de

€520 millones cada año—un incremento masivo de recursos. El total sería aún mayor si la tasa fuera incrementalmente mayor para las organizaciones más grandes[28].

PREGUNTA PARA DISCUSIÓN

1. **¿Qué caminos se podrían explorar para incrementar los presupuestos de las APDs a niveles más realistas?**

[28] En el Reino Unido hay más de 400,000 responsables registrados. La tasa para organizaciones grandes es de £500.

4. Vigilancia efectiva

El reto de la efectividad es obtener los mejores resultados con los recursos disponibles. La protección de datos no existe en el vacío y hay mucho para aprender de otras esferas regulatorias. Muchos estudios de efectividad regulatoria han sido publicados en años recientes— y la Bibliografía de este artículo menciona algunas. Desafortunadamente, dichos estudios han pasado en gran medida por encima de la protección de datos, y a su vez, quizás no han sido tomados suficientemente en serio por la comunidad de protección de datos.

Antes de discutir cómo funcionaría una Aproximación Basada en Resultados para vigilar temas de protección de datos, esta sección comenta sobre un rango de estudios significativos.

a. Temas clave

Aunque no hay un consenso universal sobre "qué funciona mejor", y el péndulo regulatorio oscila en todas las direcciones, se puede identificar una serie de temas clave. Estos incluyen:

- La práctica supervisora—el comportamiento de las autoridades—es tan importante como los contenidos de las leyes y las regulaciones.
- Apuntarle a resultados bien definidos—o vigilancia "basada en resultados"—es hoy en día reconocido como un principio regulatorio de alto nivel. En otras palabras, cualquier modelo regulatorio debería enfocarse, en la medida en que sea posible, en resultados, yendo más allá de "hacer cumplir la ley" y resistir las presiones para que se haga cumplir la ley porque sí o de imponer excesivas prescripciones regulatorias.
- Las autoridades efectivas adoptan una "aproximación basada en riesgos". Esto significa que el marco regulatorio, incluyendo la interpretación y las medidas para exigir el cumplimiento de la ley, están enfocadas en gestionar los principales riesgos frente a los objetivos regulatorios[29].
- Los reguladores efectivos seleccionan la aproximación más apropiada de una gran cantidad de herramientas diseñadas para asegurar el cumplimiento legal, involucrándose con sus regulados y prefiriendo cuando sea posible el "cumplimiento voluntario" a las medidas sancionatorias. Esta aproximación se vuelve incluso más relevante cuando se requiere a los regulados o se espera

[29] Esto es especialmente relevante en las provisiones sobre riesgo del RGPD. Ver también "A Risk-based Approach to Privacy: Improving Effectiveness in Practice", CIPL 2014, disponible en http://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_artículo_1-a_risk_based_approach_to_privacy_improving_effectiveness_in_practice.pdf; y "Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the RGPD", CIPL 2016, disponible en http://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_RGPD_project_risk_white_artículo_21_december_2016.pdf.

que adopten esquemas de responsabilidad demostrada o proactiva (*accountability*).

- También aprovechan una serie de palancas adicionales a sus propias facultades formales para asegurar que los estándares se mantengan. Estas palancas incluyen las influencias que vienen de los usuarios, consumidores y ciudadanos (especialmente allí donde pueden tomar decisiones en un mercado competitivo y en escenarios democráticos), de la presión social entre vigilados, de las redes sociales y los medios tradicionales y de la esfera política.

b. Ley y Comportamiento Corporativo

Uno de los más recientes y completos estudios profundiza sobre estos asuntos y vale la pena por tanto citarlo con mayor detalle. En su libro de 2015, *Law and Corporate Behaviour*, (Ley y Comportamiento Corporativo)[30] Christopher Hodges, profesor de sistemas de justicia en la Universidad de Oxford, llena aproximadamente 800 páginas de evidencia y análisis para aportar a la discusión sobre regulación efectiva. En los términos descritos por su propio subtítulo, se trata de "[i]ntegrar teorías de regulación, aplicación de la ley, cumplimiento y ética"[31].

El profesor Hodges ha avanzado en consecuencia el concepto de "Regulación Empresarial Ética" ("EBR" por sus siglas en inglés: Ethical Bussiness Regulation), la cual, basada en datos empíricos sobre por qué la gente cumple o viola las reglas y sobre cómo la cultura puede ayudar a un continuo mejoramiento e innovación, se intenta generar éxitos comerciales basado en el cumplimiento de valores sociales.[32]

<u>Máximo Cumplimiento Legal</u>

Hodges argumenta que la regulación se trata fundamentalmente de comportamiento. El resultado óptimo es producir comportamientos aceptables y frenar el comportamiento inaceptable. En términos prácticos, la regulación efectiva significa asegurar que se produzca el nivel máximo de cumplimiento legal.

Un cuerpo importante de evidencia demuestra cómo los reguladores en las democracias contemporáneas deben buscar cambiar los comportamientos corporativos para lograr ese máximo de cumplimiento. Esto incluye los resultados de las investigaciones sobre sicología comportamental y el análisis de los incentivos económicos y culturales. La regulación por sí misma no puede lograr el cumplimiento legal, especialmente en la medida en que está fuertemente

[30] En la página 8.
[31] Un resumen de los puntos clave está disponible en https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/497539/16-113-ethical-business-regulation.pdf.
[32] *Ethical Business Regulation; Growing Empirical Evidence*, Christopher Hodges, Wolfson College, Universidad de Oxford.

influenciada por la presión de los consumidores, el comportamiento de los competidores, los comentarios en los medios y consideraciones de tipo reputacional. Las normas sociales, los valores éticos y la presión social también juegan un papel importante. El interés propio ilustrado (*enlightenend self interest*)—donde el cumplimiento se ve como una manera de alcanzar mayores rentabilidades u otros objetivos corporativos—muy frecuentemente esun factor dominante.

La regulación efectiva implica apropiarse de estas fuerzas y otras similares, no resistirlas ni trabajar de manera aislada a ellas.

La aproximación moderna a la regulación

La esencia de una democracia moderna se basa en el respeto del otro, y se apoya entre otras cosas en la defensa de los derechos humanos fundamentales. Aplicar esa política a una economía de mercado dinámica produce como resultado que la sociedad apoye a los empresarios honestos en pro de la mejora del bien común. Las empresas honestas y las sociedades armoniosas funcionan sobre la base de la confianza. Así, un objetivo clave de la regulación debe ser su capacidad para generar confianza en las empresas, base sobre la cual se pueda desarrollar una economía sostenible y en crecimiento constante, lo que a su vez se traduce en empleo, estabilidad social e innovación. Esta filosofía es igualmente aplicable con independencia de que los objetivos regulatorios sean primordialmente económicos o sociales.

En línea con esta filosofía general, la mayoría de la regulación moderna se ha movido del modelo histórico—donde un individuo o una organización poderosa "manda y controla" las acciones de sus inferiores, ejerciendo autoridad sobre la base de castigos fuertes, reales o temidos, para aquellos que no obedecieron. Hoy en día existe un consenso universal—y usualmente vinculante y legalmente exigible—de que incluso cuando las autoridades ostenten un poder significativo para hacer cumplir la ley, deben actuar de manera justa y proporcional, respetar el debido proceso y estar listos a responder por sus actuaciones.

La aproximación moderna inevitablemente requiere también un buen entendimiento de porqué las organizaciones y las personas se comportan de determinada forma y cómo se les puede ayudar a mejorar.

La investigación empírica muestra que las personas obedecen las reglas cuando:

a. las reglas encuentran una correspondencia con el sistema reconocido de valores;

b. las reglas se han construido de manera justa; y

c. las reglas se aplican con justicia.

Regulación responsiva

Un gran volumen de investigación actual avala hoy en día la regulación “responsiva” donde el énfasis se pone en el relacionamiento a través de información, asesorías, y apoyo más que en la disuasión y el castigo. Estas investigaciones han cubierto una amplia gama de actividades reguladas, incluyendo la salud ocupacional, contaminación del agua, protección medioambiental, la industria minera, el procesamiento de alimentos, el cuidado de personas de la tercera edad y la aviación civil.

Resultados, no cumplimiento legal

En respuesta a las altas tasas de accidentes en las obras de construcción en los años 90’s, el regulador del Reino Unido (Health & Safety Executive (HSE)) decidió optar por una nueva aproximación—hacer que aquellos involucrados se *apropiaran* del problema. En vez de inspecciones uno-a-uno en miles de obras, la nueva aproximación, implicaba apalancar la influencia en áreas de alto riesgo e involucrarse y formar alianzas con las diferentes partes dentro de la industria para lograr un cambio generalizado.

Esta nueva aproximación tuvo un gran éxito. De 2000-01 a 2012-13 el número de accidentes graves y fatales en la industria bajó de 4,410 a 2,161 (49 %).

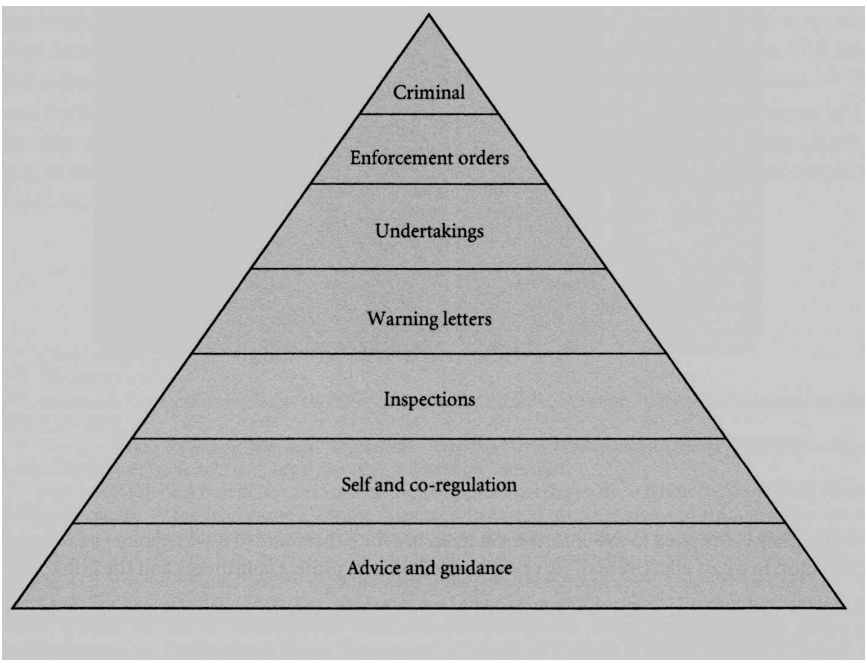
Un estudio comparando las políticas de cumplimiento de varios países con las mismas leyes, ilustraba claramente que la diferencia en efectividad no estaba en las normas, sino en la aproximación adoptada por las autoridades[33]. La aproximación del Reino Unido ha reducido permanentemente la ocurrencia de incidentes graves de seguridad. La misma aproximación se adoptó en Alemania, con el mismo resultado. La aproximación en Francia, sin embargo, todavía depende de las inspecciones y las sanciones por no cumplimiento de las normas. El juego para los empresarios es entonces aprobar las inspecciones, en vez de concentrarse en hacer que los sitios de trabajo sean seguros. El record de seguridad en el sitio de trabajo en Francia continúa siendo uno de los peores de Europa[34].

La experiencia en esta y otras áreas es muy diciente de los beneficios de una cultura donde los reguladores adoptan una aproximación positiva y proactiva hacia el logro del cumplimiento legal. Esto implica que los reguladores ejerzan sus funciones de forma que ayuden a sus regulados a cumplir. Particularmente, debe darse una prioridad alta a asegurar que haya información clara, guías y asesoría de manera permanente para ayudarle a las organizaciones a cumplir sus responsabilidades. Dicho apoyo es aún más importante para las PYMES, donde la investigación ha mostrado que muchas veces creen que están cumpliendo con la ley hasta que una persona a quien respetan (por ejemplo una autoridad o un gremio)

[33] F Blanc, *From Chasing Violations to Managing Risks. Origins, challenges and evolutions in regulatory inspections* (Edward Elgar, próximo).
[34] Ibid.

les señalan que podrían mejorar, después de lo cual normalmente siguen dicha recomendación.

Regulación Responsiva– la aproximación de la Autoridad de Aviación Civil del Reino Unido[35]



***** En la pirámide, de arriba hacia abajo: 1. Consejos y guías, 2. Auto regulación, 3. Inspecciones, 4. Cartas de apremio, 5. Órdenes, 6. Órdenes de Cumplimiento, 7. Penal.

c. Conclusiones de otras esferas regulatorias

De la evidencia y de este análisis, el Profesor Hodges saca cinco conclusiones básicas[36]:

1. **Un sistema regulatorio es más efectivo cuando es consistente y apoya aquellos comportamientos que son vistos como justos, proporcionales y éticos.**

2. **Las organizaciones deben estar en capacidad de demostrar, con evidencia, su compromiso con aquellos comportamientos que generarán confianza en los reguladores, así como en sus propios directivos y empleados, clientes, proveedores, inversionistas y otras partes interesadas.**

[35] CAA Políticas de Cumplimiento Regulatoria, basada en el modelo "responsivo" de regulación desarrollado por el Profesor John Braithwaite, tal y como se cita en *Law and Corporate Behaviour*.
[36] Estas se expanden en el Anexo C.

3. **El aprendizaje es fundamental y se promueve con un relacionamiento abierto y constructivo entre los reguladores y los regulados, pero se desincentiva con el énfasis en la "culpa" y/o el castigo.**
4. **Los sistemas regulatorios deben basarse en el diálogo y la cooperación mutua que están explícitamente dirigidos a maximizar el cumplimiento, la prosperidad y la innovación.**
5. **Allí donde las organizaciones efectivamente violen la ley, se necesita una respuesta proporcional, donde se reserven las sanciones más severas a las conductas deliberadas, reiteradas o dolosas.**

PREGUNTA PARA DISCUSIÓN

1. ¿Qué se puede aprender de las aproximaciones adoptadas alrededor del mundo en otras esferas regulatorias?

5. Una Aproximación Basada en Resultados para la vigilancia en Protección de Datos

La evidencia y el análisis contenido en varios estudios, como se sintetiza a continuación, es consistente con una corriente de pensamiento más basada en el sujeto que está empezando a surgir dentro de la comunidad de protección de datos. Tanto las APDs como las organizaciones reguladas entienden cada vez más que el cumplimiento es parte de la responsabilidad y sostenibilidad corporativa.

A medida que nuestra sociedad digital se transforma a través de la cuarta revolución industrial, un nuevo ecosistema de protección de datos está surgiendo—basado en las organizaciones responsables y en autoridades efectivas orientadas a resultados.

A nivel de la UE, hay un reconocimiento creciente de los retos fundamentales para las APDs que se pueden resumir en términos sencillos:

- Desde mayo de 2018, las funciones de las APDs se aumentarán considerablemente;
- Los recursos de las APDs son escasos para sus funciones y serán inadecuados para cumplir con toda la gama de tareas prescritas por el RGPD;
- Hay pocas o ninguna perspectiva de aumentos suficientes por parte de los gobiernos; e
- Incluso los aumentos significativos no evitarán la necesidad de adoptar aproximaciones estratégicas.

Las bases de la responsabilidad demostrada o proactiva organizacional como un motor del cumplimento legal en protección de datos, que CIPL articuló por muchos años y que fue reconocida con autoridad en la importantísima opinión sobre Responsabilidad Proactiva (Accountability) por el GT29,[37] ahora se encuentra en el corazón del RGPD. La Responsabilidad Proactiva (Accountability) es también esencial en las Guías de Privacidad de la OCDE. Globalmente, las guías sobre gestión de programas integrales de protección de datos de las autoridades de Canadá, Hong Kong y Australia han sido muy bien recibidas e influyentes, así como las referencias a la responsabilidad Proactiva en las leyes de Colombia y México

En 2015, el Supervisor Europeo de Protección de Datos (SEPD) publicó una Opinión, *Hacía una nueva ética digital*,[38] que dio seguimiento a las actividades del SEPD, promoviendo sinergias con las leyes de consumidor y de competencia[39]. La Opinión de 2015 contempla un régimen efectivo de protección de datos en términos de un "ecosistema" donde todos los jugadores relevantes (pero especialmente las APDs y los Responsables) actúan conjuntamente para reforzar los derechos.

[37] Opinión 3/2010 sobre el principio de responsabilidad demostrada, WP 173.
[38] Opinión 4/2015 del SEPD.
[39] Por ejemplo: https://secure.edps.europa.UE/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2014/14-03-26_competitition_law_big_data_EN.pdf

La importancia de un interés propio ilustrado (*enlightened self-interest*) como un motor del comportamiento corporativo ha sido explícitamente explorado por la anterior comisionada interina de privacidad de Canadá. El artículo de discusión publicado por Chantal Bernier[40] plantea como el concepto de la "Licencia Social para Operar"" (LSO) podría convertirse en la "mejor herramienta de cumplimiento de las leyes de protección de datos". Aquí se plantea cómo convertir la aceptación social en el denominador común entre autoridades y empresas, especialmente en la medida en que los individuos sean más asertivos en sus expectativas y las empresas empiecen a preocuparse por el impacto en sus estados de resultados de su reputación en materia de gestión de datos.

Recientemente, un reporte[41] publicado por la Cámara de Comercio de los Estados Unidos en febrero de 2017 argumentó que los riesgos y retos de la protección de datos que se desprenden de la ubicuidad y el valor creciente de la información personal en la economía global hacen que sea imperativo entender cómo regular la protección de datos de forma efectiva. Un estudio de las APDs alrededor del mundo demuestra, sin embargo, que "sus metodologías, prácticas y rango de funciones varían de forma significativa". El reporte concluye que "...el denominador común entre todas las APDs es que las APDs realmente efectivas tratan a sus vigiladas como socios en vez de como rivales". Con una aproximación que se corresponde con el análisis y las sugerencias de este artículo de CIPL, el reporte identifica siete Atributos Clave para una efectiva gobernanza en protección de datos. Estos ponen un énfasis grande en educación, concientización, retroalimentación, guías y asistencia.

a. Efectividad

No se ha fijado un consenso sobre qué significa la efectividad en un contexto de protección de datos. En un nivel general, frecuentemente se hacen referencias a conceptos como "garantizar los derechos fundamentales de los individuos", "alcanzar un nivel alto de protección de datos" o "asegurar el cumplimiento de los requerimientos legales". Pero esas aspiraciones pueden sonar vacuas sin unos objetivos más concretos. Igualmente, las referencias a riesgos, prioridades, objetivos y mantras como "selectivos para ser efectivos" no significan mucho salvo que haya claridad y acuerdos sobre qué significa ser "efectivo".

Como punto de partida, todas las autoridades efectivas deben preguntarse:

- "¿Qué resultados estamos tratando de alcanzar?".
- "¿Qué significa 'ser exitoso'?".
- "¿Cómo sabremos que hemos hecho un buen trabajo?".

[40] The Concept of Social Licence to Operate: A Common Ground to Apply Privacy Law? - Dentons, Ottawa.
[41] *Seeking Solutions*, Cámara de Comercio de EE.UU, febrero de 2017, https://www.uschamber.com/sites/default/files/023052_dataprotectionhuntonartículo_fin.pdf.

CIPL no tiene las respuestas a estas preguntas, que, en todo caso, deben ser respondidas y acordadas por las APDs entre ellas mismas, sea colectiva o individualmente. El objetivo básico de proteger a los individuos ya se ha mencionado, pero, como sucede con la protección del medio ambiente, hay una dimensión más amplia del "bien social". En el taller que CIPL llevó a cabo en Dublín emergió un consenso amplio sobre la importancia de buscar y asegurar resultados claramente articulados, más que el cumplimiento por el simple cumplimiento. También se reconoció que una regulación fundamentalmente efectiva involucra monitorear y cambiar comportamientos, y a veces culturas, no solamente asegurar que las formalidades y la documentación estén en orden.

En ese sentido, más allá del mero cumplimiento, la supervisión en protección de datos implica apuntarle a un mundo digital donde la gente se desarrolle con dignidad en su dimensión de individuos autónomos. Los resultados generales que se buscan podrían entonces desarrollarse en las siguientes líneas:

- la prevención de los usos de datos que menoscaben la calidad de vida de los individuos mediante la negación de la privacidad a la que tienen derecho; y
- la promoción de una sociedad donde una buena calidad de vida para los individuos fluya de una privacidad genuina y generalizada donde los usos de datos en un mundo digital sean al mismo tiempo universales y populares.

Debemos enfatizar, sin embargo, que deben ser las propias APDs quienes articulen los resultados que están buscando.

b. Definiendo prioridades estratégicas

Cualquier APD bien manejada tendrá que definir prioridades claras, usualmente en un plan estratégico que sea transparente. Si las prioridades no se articulan de forma explícita, podrá no obstante hacer una priorización *de facto* materializada en el trabajo hecho y el que le quede sin hacer. La Resolución de la Conferencia mencionada anteriormente reconoce la necesidad de una aproximación priorizada:

- "No es sin embargo sólo una cuestión de recursos. También es necesario que las Autoridades de Protección de Datos adopten una aproximación sostenible sobre cómo ejercer sus funciones, a nivel nacional, de la UE y europeo, apuntándole a las actividades donde la necesidad de proteger la privacidad sea más alto…".

Esto no es sencillo de llevar a cabo. Usar el lenguaje común de "priorizar" o adoptar una "aproximación basada en riesgos" es relativamente sencillo, pero mucho más difícil será ir más allá de la retórica y desarrollar criterios significativos, principios u otras medidas para determinar las prioridades, los objetivos y los riesgos que se deben afrontar. Esto aplica por lo menos en dos dimensiones:

- ¿Cómo debe hacerse el ranking de funciones (o tareas o actividades)?

- ¿Cómo se le debe apuntar a sectores, actividades u organizaciones para que encuadren dentro de alguna de las funciones?

Todas las autoridades regulatorias, en todos los sectores y jurisdicciones, enfrentan estas preguntas. La evidencia de otras esferas regulatorias, como se resumió en la sección anterior, sugiere cómo se está contestando. Hay lecciones que son aplicables a la protección de datos personales. En particular, existe un cuerpo considerable de evidencia que puede ayudar a guiar el proceso de definición de prioridades.

El siguiente razonamiento podría ser útil para contestar estas preguntas:

PREDECIR - PREVENIR- DETECTAR - SANCIONAR

Estos son los objetivos claves para cualquier autoridad, pero es necesario decidir cuál será el balance adecuado entre ellos y dónde establecer las prioridades. La evidencia de otras esferas regulatorias sugiere que “Prevenir” debe ser lo primordial, con el apoyo de “Sancionar” cuando sea necesario. Después de esto se puede desarrollar una estrategia relacionando esos objetivos con todas las funciones de las APDs.

Una aproximación a la vigilancia basada en resultados, implica el mayor grado posible de relacionamiento con las organizaciones vigiladas y, como lo demuestra el cuadro siguiente, el Liderazgo es crucial para alcanzar de forma efectiva todos los objetivos:

	Líder	**Autorizador**	**Oficial de Policía**	**Gestor de quejas**
PREDECIR	✓			
PREVENIR	✓	✓		
DETECTAR	✓		✓	✓
SANCIONAR	✓		✓	✓

Este análisis también sugiere un ranking amplio de prioridades:

1. **“Líder”** – donde el énfasis está en la experticia, autoridad, influencia e información proveída por la APD.
2. **“Oficial de policía”**– donde el énfasis está en sancionar en aquellos casos en que ha habido, o podría haber, una violación de la ley.

3. **“Gestor de Quejas”** – donde el énfasis está en lidiar con las quejas de los individuos, que pueden llevar directa o indirectamente a una sanción o a una compensación.
4. **“Autorizador”** – donde se requiere algún tipo de autorización previa por parte de la APD.

c. Liderazgo y Relacionamiento

> “Las guías que las APDs produzcan hoy, producirán los resultados esperados el día de mañana”.

Debería ser incontrovertible desde este análisis que el rol de liderazgo –guiar las buenas prácticas—es la prioridad número uno y está llamada a crecer cada vez más en importancia en la era moderna de la información. Atraviesa todos los objetivos que deben alcanzarse.

El liderazgo abarca todas aquellas funciones que dependen de la experticia y la autoridad de la APD. Una APD efectiva querrá ser, y además ser vista como, la líder en hacer claros los resultados y comportamientos que espera se alcancen. Esto implica entender los ambientes tecnológicos, comerciales y políticos, anticipar los temas, interpretar la ley y proveer guías que sean avanzadas, prácticas y estratégicas. Aun cuando juegan un papel aquí, este no es un rol que se pueda delegar a los abogados, consultores u otros asesores, ni dejarse en las manos de los vigilados mismos. Es fundamental que las APDs se ***involucren*** directamente en el diálogo y asuman el liderazgo en proveer la información, asesoría y apoyo que harán de la protección de datos una realidad práctica. Las APDs pueden apalancar los insumos de las organizaciones vigiladas, tanto en el sector privado como en el público, para ayudarles al cumplimiento de su misión.

El relacionamiento requiere confianza mutua y refuerza el principio de Responsabilidad Proivaact (*Accountability*) del RGPD. Es un proceso de doble vía—donde las organizaciones responsables desearán y estarán en capacidad de demostrar el cumplimiento, ser transparentes sobre sus propias actividades y compartir su visión sobre innovaciones y tendencias tecnológicas y comportamentales. Aunque el liderazgo fundamentalmente debe involucrar diálogo con los vigilados, la información, la asesoría y el aumento de la concientización para el público también juegan un papel importante.

Ejemplos de relacionamiento de una APD

- El GT29 ha tomado la muy bienvenida iniciativa de abrir a consultas sobre los borradores de las Opiniones y Guías antes de su adopción. Los ejemplos recientes incluyen las de autoridades principales, portabilidad de datos y Oficiales de Protección de Datos.

- Una serie de APDs han discutido asuntos de Inteligencia Artificial con empresarios del sector y ahora están reconociendo que una aproximación que pida "transparencia de algoritmos" podría ser menos productiva que un énfasis en "Accountability de IA y revisiones específicas".

- Los "FabLabs", organizados por el GT29 para discutir la implementación del RGPD, han sido muy apreciados.

- El SEPD ha estructurado un programa de alto nivel para instituciones de la UE supervisadas por este. Estas frecuentemente resultan en una hoja de ruta para alcanzar el cumplimiento "voluntario" lo cual evita la necesidad de sanciones o procedimientos formales[42].

- El SEPD también consulta regularmente a los OPDs sobre los borradores de las Guías.

- La iniciativa *Pack de conformité* de la CNIL ha invitado a compañías de determinados sectores a definir con la CNIL las mejores prácticas de protección de datos para dicho sector y además simplificar las formalidades administrativas.

- La FTC en EE.UU. hace talleres y consultas temáticas regularmente, sobre desarrollos tecnológicos específicos o temarios avanzados, para solicitar retroalimentación e intercambiar aprendizajes con expertos, académicos y líderes claves.

- Las APDs que participan en las reuniones bianuales de APPA frecuentemente invitan a representantes de las organizaciones vigiladas a intercambiar puntos de vista en temas clave de interés para las autoridades.

De manera creciente, las APDs están reconociendo los beneficios de la colaboración y el relacionamiento con las organizaciones vigiladas, especialmente aquellas que buscan una aproximación responsable al cumplimiento legal. Aun cuando hay por supuesto muchas "zonas grises", es ampliamente reconocido que unas pocas organizaciones buscan evitar cumplir con la ley. Aunque muchas organizaciones, especialmente PYMEs, pasan trabajos debido al desconocimiento, la mayoría aceptan que deben cumplir con sus obligaciones legales. Muchas de las organizaciones más grandes, han creado programas de gestión de datos personales

[42] Ver los Informes Anuales Sucesivos del SEPD.

para lograr una “auto-confianza efectiva” o un “reconocimiento merecido”, y en cosnecuencia se ha alejado del síndrome tradicional de “papeleo de protección de datos” donde los esfuerzos pocas veces iban más allá de una serie de políticas que se llenaban de polvo en un escritorio. Estas tendencias encuentran apoyo en el RGPD con su énfasis en Responsabilidad Proactiva (*Accountability*) y Gestión de Riesgos y su promoción de los esquemas de certificación y sellos de confianza. Como mínimo, un programa integral de protección de datos debería contener evidencias concretas de esfuerzos serios para alcanzar el cumplimiento legal.

Una parte adicional del rol de liderazgo de las APDs es alentar a las organizaciones para que adopten marcos de responsabilidad proactiva e incentivar los buenos comportamientos. Esto se puede hacer ofreciéndoles formalmente mitigaciones a aquellas organizaciones que sean capaces de demostrar una responsabilidad proactiva continuada, o simplemente mediante el reconocimiento de aquellos ejemplos de mejores prácticas que ayuden a crear *momentum* de mercado y presión de grupo para que los demás sigan ese ejemplo. Por ejemplo, el PDPC de Singapur, aprovechando una importante conferencia internacional y la semana de Protección de Datos de Singapur en 2016, distribuyó un folleto que en términos didácticos mostraba las mejores prácticas de más de media docena de organizaciones en Singapur, que iban desde grandes multinacionales, pasando por entidades del sector público y emprendimientos locales.

Al mismo tiempo, las APDs necesitan sofisticar más sus estrategias. Por ejemplo, deberían entender los Principios y la lógica de la gestión de riesgos y el continuo mejoramiento de las políticas y procedimientos de cumplimiento, y no usarlos para mostrar debilidades, que pueden haber sido abiertamente reconocidas por las organizaciones, pero tratados como asuntos de prioridad baja de manera justificada. Igualmente, las guías de las APDs sobre actividades de bajo riesgo o *de minimis* seguramente serán bien recibidas como parte de una aproximación basada en riesgos.

d. Oficial de policía

El rol de Oficial de Policía (investigando, amenazando o embarcándose en acciones formales contra organizaciones que no cumplen con la ley), es importante, pero si se buscan resultados serios de cambios comportamentales, no debería ser la prioridad prevalente para ninguna APD. Las evidencias que se resumen en la sección 4 anterior sugieren que dicha actitud sería tanto inefectiva como contraproducente. Existen riesgos significativos de que los vigilados adopten actitudes defensivas, secretas o abiertamente hostiles que poco servirán para mejorar los resultados para aquellos a quien se supone protegen. Los recursos escasos fácilmente podrían terminar desviándose hacia la defensa de largas batallas legales en los tribunales. Ninguna autoridad puede pretender ser efectiva si su primera aproximación es propagar el miedo.

Esto de ninguna manera significa negar el importante rol que juega el hacer cumplir la ley. Las APDs alrededor del mundo han sido dotadas en los últimos años de dientes mucho más afilados, muy notablemente en el RGPD que introduce multas de hasta 20 millones de euros o 4 % de los ingresos mundiales anuales. Dichas sanciones incrementan la credibilidad y la legitimidad y enfocan la mente. La posibilidad de que se ejerzan las capacidades sancionatorias junto con sanciones más fuertes indudablemente influenciará a muchas organizaciones, especialmente en aquellos casos donde puedan generarse daños comerciales o reputacionales. Las APDs tendrán que ejercer sus capacidades de investigación cada cierto tiempo para que sean representativas, por supuesto teniendo en cuenta criterios de proporcionalidad. Cuando se tomen acciones decisivas, especialmente si está involucrada una multa cuantiosa, será fácil llamar la atención (entre otros por conducto de los medios o canales políticos)

Algunos incidentes de seguridad (o quiebras de seguridad) pueden ser tan graves que una sanción es inevitable. Sin embargo, claramente los objetivos más obvios para las acciones investigativas deben ser aquellas organizaciones que están llevando a cabo actividades deliberadas, conscientes, reiteradas o en grave incumplimiento de la ley (y eso además se puede definir como un objetivo explícito). Esta aproximación es consistente con el RGPD, que incluye múltiples factores que deben tenerse en cuenta cuando se decide si se multa o no, así como el monto de la sanción. Estos factores incluyen la gravedad de la infracción, su carácter intencional o negligente, así como cualquier violación previa de la ley[43]. En la mayoría de los casos, es conveniente dar algún tipo de advertencia, tanto para alertar a la organización como para facilitarle a la APD demostrar la culpa o el dolo. Si una APD quiere ser un Líder exitoso, el uso del “palo” es algo razonable, especialmente en aquellas situaciones donde se han ignorado las advertencias sobre comportamientos violatorios de la norma y existe un riesgo real de que se genere un daño a los individuos.

e. Gestor de quejas

Aunque la ley de la UE considera los mecanismos de quejas como un elemento importante del derecho del titular a la protección de datos, y la gestión de quejas se encuentra incluida en algunas leyes de protección de datos alrededor del mundo, es inusual en otras esferas regulatorias que la autoridad también tenga funciones de gestión de quejas.

En la UE, el RGPD especifica que es obligatorio que las APDs “gestionen” quejas. Esto no es nuevo y, bajo la ley actual de la UE, las quejas se deben atender con diligencia, punto que se encuentra en la médula del caso *Schrems*[44].

[43] RGPD, Artículo 83(2).
[44] Caso C-362/14, Schrems, UE:C:2015:650.

Sin embargo, es probable que se presenten serios problemas y amenazas a la efectividad si el rol de Gestor de Quejas recibe una prioridad excesiva y no se gestiona eficazmente. Como primera medida, este rol está definido por la demanda—por fuera del control de las APDs—y puede ser muy intensivo en términos de recursos, en detrimento de otras funciones. A menos que los casos se escojan de manera muy cuidadosa, puede distraer de actividades más estratégicas y (aun cuando se gestione bien) la gestión masiva de quejas rara vez producirá los comportamientos deseados en un sector determinado. En vez de concentrarse en mecanismos para resarcir a unos pocos individuos, o numerosos (pero pocos en términos relativos), las autoridades deberían concentrarse en proteger los derechos de forma más universal antes de que se generen los daños. Hay riesgos reales de que se cree un ambiente de decepción o desilusión público—a través de backlogs o de resultados indeseados—y de que se pierda el apoyo popular que las APDs necesitan.

Esto no significa que el rol de Gestor de Quejas deba –o pueda- ser ignorado totalmente. El RGPD impone un deber a las APDs de “gestionar e investigar” las quejas. Pero esto puede implicar una discreción amplia. “Gestionar” es un concepto flexible que no se desarrolla de manera extensa. El artículo 57(1)(f) del RGPD requiere que la investigación se haga “con el alcance necesario”, lo que ciertamente deja un campo para una gestión priorizada, diferenciaciones entre los distintos tipos de quejas, prioridad para los casos más graves y traslados cuando sea necesario

Una Aproximación Basada en Resultados debería involucrar varios elementos con relación a las quejas:

- el rol de Gestor de Quejas se debe administrar bien para evitar que la APD termine desbordada;
- las APDs deben ser conscientes de los riesgos generales frente a la efectividad que se pueden derivar de un uso ineficiente de los recursos;
- se debe resaltar el valor de las quejas como una fuente e inteligencia;
- las peticiones y solicitudes de información se deben separar de las quejas en sentido estricto;
- se deben desarrollar criterios objetivos para determinar qué quejas se van a “gestionar e investigar” más allá de su revisión y monitoreo inicial;
- se deben introducir procedimientos consistentes de trámite (*triage arrangements)* robustos para asegurarse que los criterios se apliquen de manera consistente y justa;
- las APDs deben poder identificar rápidamente las quejas abusivas, frívolas o vejatorias;

- se deberían promover en los quejosos (o dirigirlos a, cuando sea del caso) los mecanismos alternativos de solución de conflictos (MASC)[45] que puedan llevar a soluciones;
- se debería alentar a los quejosos a dirigirse primero a la organización implicada, la cual, como una organización responsable (*accountable*) deberá tener políticas de gestión de quejas y estar en capacidad de atenderlas en debida forma; y
- se deberían promover los programas de certificación y sellos de confianza para proveer acuerdos de resolución de conflictos a través de terceros.

Todo lo anterior aliviaría las cargas de las APDs que tienen que lidiar con un gran número de quejas que se podrían resolver mejor directamente en la fuente o a través de MASC. Esto le permitiría a las APDs concentrarse en quejas más graves o en aquellas frente a las cuales la organización involucrada no dio una respuesta satisfactoria.

Las APDs deberían, en cualquier caso, publicar sus políticas sobre gestión de quejas. Con dicha aproximación, y en línea con los Principios de "alcance adecuado" y "debida diligencia", se puede dar una atención más detallada, por ejemplo, a aquellas quejas que:

1. de forma acumulada, sugieran un incumplimiento generalizado que afecte a muchas personas;
2. sugieran un detrimento particularmente grave;
3. informen sobre incumplimientos graves y continuados;
4. puedan conducir a mejoras esenciales en el comportamiento organizacional; o
5. sugieran que hay un punto importante relacionado con algún principio que se deba abordar.

Una aproximación de este tipo resulta en un uso eficiente de los recursos escasos y además se usan las quejas como una fuente de inteligencia para complementar y apoyar otras funciones más importantes. Al mismo tiempo, con esto se genera claridad de que las APDs no pueden permitirse distraerse en ofrecer un servicio de resolución de quejas en volúmenes altos que está determinado por la demanda.

Una objeción a la aproximación descrita anteriormente puede ser el potencial impacto en el derecho de los individuos a una protección efectiva de su derecho. El derecho a la protección de datos es un derecho que los individuos deberían poder ejercer de forma efectiva. CIPL sugiere, sin embargo, un mayor énfasis en mejorar la conducta organizacional. Esto, en efecto, mejoraría la sustancia de este derecho mediante la mejora de la efectividad de las leyes de protección de datos en general

[45] Ver también la relatividad del nuevo marco europeo de resolución alternativa de conflictos de consumidor (CADR).

(como el Tribunal de Justicia de la Unión Europea enfatizó en Costeja)[46]. Es importante recalcar que la ley de protección de datos muchas veces es vista, como la protección ambiental, como un bien público que beneficia a todos. En un ambiente más estratégico, otros métodos de protección también podrían jugar un rol importante para asegurar protecciones efectivas para el individuo.

Debida diligencia en el contexto de la UE

En *Schrems*[47]*,* el Tribunal de Justicia de la Unión Europea decidió que las APDs deben examinar las quejas de los individuos relacionadas con su derecho a la protección de datos "con toda la debida diligencia". Aun cuando el significado de debida diligencia no es totalmente claro, puede argumentarse que "debida diligencia" implica que todas las quejas deben ser investigadas por la APD, de forma apropiada a la queja. El requerimiento de debida diligencia es esencialmente un compromiso entre un amplio margen de discreción que tienen a su disposición las APDs y la protección de los quejosos. Las APDs, teniendo recursos limitados, deben asegurar un alto nivel de protección, pero también proveer una solución legal para aquellos que alegan que en su caso individual se infringió la ley. La debida diligencia podría funcionar como un compromiso, bajo el entendido de que no se interprete como una obligación para dedicar recursos para investigar todas las quejas. El valor agregado de una APD independiente no es solo su amplio rango de tareas, sino también su capacidad para llevar a cabo estas tareas de la manera que lo considere más efectivo.

f. Autorizador

El rol de la APD como Autorizador también es en gran medida dictado por la demanda, potencialmente intensivo en recursos y no estratégico.

Cubre aquellas situaciones donde se necesita alguna forma de consulta formal, autorización previa o aprobación por parte de la APD. Esta aproximación *ex ante* significa que las actividades involucradas no se pueden llevar a cabo en absoluto sin dicha autorización. Los ejemplos en el RGPD incluyen las aprobaciones de BCR (Normas Corporativas Vinculantes, en inglés *Binding Corporate Rules*), contratos ad hoc para transferencias de datos, consultas previas en los casos de las Evaluaciones de Impacto de Protección de Datos (EIPD) donde no se pueda mitigar el riesgo, códigos de conducta, etc. Los procesos actuales de autorización pueden no contribuir mucho a la efectividad entendida en términos de alcanzar estándares más altos de comportamiento. Aun cuando los volúmenes son difíciles de predecir, esta puede ser una función significativamente intensiva en términos de recursos, especialmente si cada aplicación se considera individualmente y de forma detallada.

[46] Caso C-131/12 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González*.
[47] Caso C-362/14, Schrems, UE:C:2015:650, at 63.

De la misma manera como sucede con la gestión de quejas, esta función en sí misma, así como su razón de ser, no se pueden ignorar. Sin embargo, hay campo para que las APDs consideren cómo simplificar y descargar esta función de forma efectiva, especialmente cuando se trata de tratamientos internacionales que caen dentro del ámbito de la ventanilla única y los procedimientos de consistencia. El CEPD podría jugar un rol determinante en este campo, mediante la expedición de guías, recomendaciones y mejores prácticas como las previstas en el Artículo 70(1) del RGPD, de forma que también logren un relacionamiento con las APDs que se encuentran fuera de la UE.

De nuevo, es necesario acudir a una aproximación estratégica y de cooperación. El uso de algún tipo de aprobación "basada en categorías" para ciertos tipos de actividades prescritas, quizá de forma paralela con que estén presentes las condiciones adecuadas, podría ser prometedor[48]. Para cada caso donde se necesite autorización, esta fácilmente podría darse sobre la base de criterios publicados para la actividad. El cumplimiento de los criterios y de cualquier condición llevaría a una autorización rutinaria y automática a menos que la actividad involucre características inusuales o excepcionales. Esto se podría vincular con la aproximación de "Cumpla o Declare" usada cada vez más en otras áreas regulatorias. En la medida que la APD Líder aumente su relacionamiento con los vigilados responsables, existirá un margen considerable para consultar sobre la sustancia y aplicación de los criterios e incluso para los mecanismos de auto-certificación, que pueden ser revisados post facto por las APDs o por terceros acreditados. Obviamente, esto no reemplaza la aprobación previa específicamente requerida por la ley, pero sí alivia de manera significativa el procedimiento.

[48] Esto podría evolucionar en forma similar a las "excepciones por categoría" de la ley de competencia de la UE.

PREGUNTAS PARA DISCUSIÓN

1. **Cuando los retos y las expectativas de la era digital son tan grandes, y especialmente cuando los recursos son limitados ¿cuáles son las formas de trabajar más exitosas para que las APDs (de forma independiente y con otros) se aseguren de que la vigilancia en datos personales producirá los mejores resultados?**

2. **¿Puede elaborarse sobre el concepto de efectividad en términos de permitirle a los ciudadanos desarrollarse con dignidad y autonomía en un mundo digital donde se previenen los usos inaceptables de los datos personales?**

3. **Cuando las responsabilidades de la mayoría de las APDs son tan numerosas, ¿cuáles son las mejores formas de lograr una efectividad real?**

4. **¿La Aproximación Basada en Resultados ofrece formas útiles de establecer prioridades estratégicas y para alcanzar un balance entre relacionamiento, sanciones y gestión de quejas?**

5. **¿Es correcto darle una prioridad estratégica de alto nivel a las funciones de liderazgo con un énfasis fuerte en el relacionamiento constructivo con los sujetos vigilados?**

6. El Relacionamiento Constructivo en la práctica

El análisis en las secciones siguientes sugiere que las funciones de Liderazgo de las APDs se debería tratar como la prioridad estratégica fundamental, con tanto relacionamiento constructivo como sea posible entre las APDs y sus vigilados. En la UE esto implica reconocer el Artículo 57(1)(d) del RGPD que implícitamente reconoce que ambas partes podrían hacer mucho para ayudarle a la otra a lograr resultados regulatorios óptimos.

Esta conclusión central fue apoyada en el taller llevado a cabo en junio de 2017 en Dublín por CIPL, donde también se enfatizó el interés mutuo de las autoridades y las entidades vigiladas de lograr una supervisión y regulación real de protección de datos al tiempo con innovación de datos y un crecimiento de la economía digital. En otras palabras, las autoridades efectivas y orientadas a resultados, y las organizaciones responsables, pueden trabajar más las unas con las otras como dos pilares esenciales de la moderna protección de datos.

> "Si las empresas nos muestran [a una APD] que están invirtiendo en mecanismos de cumplimiento, nos relajaremos – a menos que veamos un incidente grave".
>
> "La clave es la confianza. Las autoridades y los vigilados deberían tener los mismos objetivos".
>
> "Hace una diferencia enorme—y el sujeto resulta tenido en cuenta de verdad—cuando las autoridades abiertamente reconocen los buenos esfuerzos y los éxitos en protección de datos".
>
> "Nosotros ya trabajamos con los empresarios para mejorar sus comportamientos. Recibimos 100,000 llamadas de PYMEs el año pasado".
>
> Participantes en el Taller de CIPL en Berlín

El taller siguió con consideraciones sobre qué es lo que el relacionamiento constructivo realmente implica en la práctica. Ya se ha empezado a ver una tendencia creciente y muy bienvenida hacia el relacionamiento constructivo por parte de muchas APDs alrededor del mundo; esto es algo sobre lo que se puede construir. Se pueden identificar muchas actividades y técnicas (tanto actuales como prospectivas):

- **Máxima transparencia** – Las APDs deberían ser transparentes en la definición de sus prioridades, expectativas y métodos de trabajo, lo que a su turno les ayudará a ser efectivas y a ayudarle a las organizaciones a "acertar desde el principio". De la misma forma, las organizaciones deben estar

preparadas para ser transparentes con las APDs, sin temor y sin la amenaza de la auto incriminación.

- **Guías prácticas**– Usualmente en formatos web, las guías deben ser sobre las interpretaciones y aplicaciones de los requerimientos regulatorios, y abiertas a consultas y comentarios por parte de las organizaciones vigiladas. La mejor guía es aquella que se hace en lenguaje simple, con muchos ejemplos y segmentada por sectores para máxima facilidad de consulta—ej. pequeños empresarios, empresas medianas, sectores específicos, multinacionales, entidades públicas, etc.
- **Participación activa**– En reuniones abiertas y cerradas, para comunicar tanto las preocupaciones como las expectativas, la participación puede ser igualmente importante para encontrar incertidumbres, tendencias, desarrollos comerciales y tecnológicos, etc.
- **"Autoconfianza vigilada"** – Se pone todo el énfasis en los OPDs, códigos de conducta, esquemas de certificación, la capacidad de demostrar la responsabilidad, etc.; la promoción del auto cumplimiento al tiempo que se reduce la presión sobre las APDs.
- **Máximo nivel de consulta,** con una aproximación "Sin Sorpresas"; por ejemplo, se buscan puntos de vista sobre proyectos de guías o retroalimentación sobre un plan determinado antes de su implementación. Dicho diálogo es esencialmente beneficioso allí donde hay requerimientos nuevos o no existen puntos de vista en común sobre qué es "lo correcto" para cumplir, o incluso qué se debería prevenir.
- **Intercambios francos**– una disposición a participar en discusiones confidenciales, muchas veces con un líder del mercado, sobre las implicaciones y la aceptabilidad –o no- de una innovación tecnológica.
- **Explotación del efecto rebaño**– De manera creciente, las APDs están reconociendo que las organizaciones tienden a seguir a un líder de la manada. Si una o dos empresas reciben algún tipo de respaldo o autorización de manera notoria para seguir un curso de acción deseable, los competidores, pares y muchos otros (especialmente PYMEs) seguirán el *benchmark* y harán lo mismo. Hay un campo importante para que las APDs exploten esta tendencia—promoviendo mejores prácticas, dándole visibilidad a los formatos de transparencia, EIPDs y otros, mostrando las mejores prácticas de organizaciones proactivas (campañas de entrenamiento o concientización, liderazgo del OPD, etc.), influenciando de forma deliberada a los asesores legales y consultores y promoviendo ejemplos de buenas prácticas en-línea.
- **Incentivos**– Los líderes corporativos se tomarán la protección de datos y la privacidad con más seriedad si las APDs pueden crear y comunicar los incentivos para los programas de privacidad y cumplimiento hechos de buena fe. Estos incentivos pueden incluir la posibilidad de compartir información a través de las fronteras, de involucrarse más activamente en actividades de

big data y machine learning y, crucialmente, de incentivos de mitigación de sanciones en caso de que se adelanten investigaciones.

- **Creación de espacios para la Innovación Responsable** – Hay un espacio considerable para la creación de soluciones de cumplimiento de forma colaborativa. El *Sandbox Regulatorio* (ver descripción más abajo)[49] ofrece una posibilidad. "Pensamiento de Diseño", donde la los requerimientos de protección de datos y los retos de cumplimiento se pueden escalar y desarrollar de abajo hacia arriba por equipos multifuncionales, puede ofrecer otras oportunidades para la participación de las autoridades y para promover el debate con las organizaciones vigiladas y con expertos de otras áreas (economistas del comportamiento, diseñadores centrados en el usuario, ingenieros de tecnología, y expertos en marketing y relaciones con los consumidores)[50].
- **Cumplimiento reiterativo y dinámico** – Tal y como sucede con el desarrollo de tecnología y software, sería útil si tanto las APDs como las organizaciones vigiladas se pudieran aproximar al cumplimiento como un proceso reiterativo y dinámico, y no como un evento que se lleva a cabo una única vez. El cumplimiento dinámico es particularmente apropiado para la protección de datos, dada la velocidad de los desarrollos tecnológicos y la adopción de soluciones digitales. Permite las mejoras, basadas en retroalimentación de los usuarios, los desarrollos internos y externos y los aprendizajes de la industria y las autoridades. Las organizaciones se deberían incentivar para que adopten el cumplimiento dinámico y las APDs no deberían castigar a aquellos que de forma activa tratan de hacer las cosas bien de manera continua.
- **Los indicadores de rendimiento** son esenciales para medir y demostrarle a las APDs el éxito en lograr influenciar directamente la proliferación de buenas prácticas preferiblemente con métricas comunes y/o comparables.

El Sandbox Regulatorio–Un espacio para la innovación responsable

El relacionamiento constructivo incluye crear un espacio para la innovación responsable por parte de las organizaciones proactivas. ¿Cómo puede lograrse esto?

El modelo de "Sandbox Regulatorio" que está siendo desarrollado por la Autoridad de Conducta Financiera del Reino Unido[51] (FCA) puede ser una forma interesante de permitirle a las compañías vigiladas experimentar e innovar en un "espacio

[49] Nota de la traducción: *Regulatory Sandbox* se refiere a un espacio seguro. En el texto se usará el término Sandbox Regulatorio, por la mayor difusión del término en inglés.
[50] Un ejemplo actual de una iniciativa de innovación responsable es el "Design Jam" de Facebook que busca nuevas aproximaciones y soluciones en pro de una mayor transparencia y control del usuario.
[51] https://www.fca.org.uk/firms/regulatory-sandbox.

seguro” con supervisión de la autoridad regulatoria.

El Sandbox Regulatorio permite a los empresarios ensayar productos, servicios, modelos de negocios y mecanismos de entrega en el mercado real y con consumidores reales.

El sandbox es un “espacio supervisado” que presuntamente otorga a las organizaciones:

- Un menor tiempo para entrar al mercado con costos potencialmente menores; y
- salvaguardas apropiadas para el consumidor que se integran directamente en los nuevos productos y servicios.

El sandbox ofrece herramientas tales como autorizaciones restringidas, guías individuales, exenciones y comunicaciones sobre salvaguardas. El FCA monitorea de cerca los ensayos usando un ambiente regulatorio a la medida para cada piloto.

Se espera que los ensayos del Sandbox tengan un objetivo claro (ej. reducir los costos a los consumidores) y que se lleven a cabo a pequeña escala, de forma que las firmas puedan ensayar su innovación por un periodo de tiempo y con un grupo de consumidores limitado. Es debatible que las innovaciones técnicas tengan un mayor impacto en la protección de datos que los servicios financieros. Este modelo puede ser particularmente útil y bien recibido por la comunidad de protección de datos, donde hay un creciente reconocimiento de que el cumplimiento debe ser abordado como un proceso iterativo.

El posible uso de este modelo de sandbox en este contexto fue sugerido por el ex secretario general de la CNIL en un artículo en *Les Echos* a principios de 2017[52].

Más recientemente, en julio de 2017, se anunció que la PDPC de Singapur está preparada para trabajar con compañías responsables y proactivas para crear sandboxes regulatorios para probar cambios legislativos que se hayan propuesto y que les permitan a las compañías continuar siendo innovadoras y competitivas[53].

El diálogo constructivo debe ser un proceso de doble vía, con un gran componente de confianza, compromiso y respeto mutuo entre las APDs y las organizaciones responsables. A menos de que las organizaciones tomen un enfoque positivo en ayudarles a las APDs a alcanzar un mejor entendimiento del panorama que están vigilando, no pueden pretender que las APDs sean abiertas y comprensivas. Las empresas vigiladas y las entidades públicas deben estar listas para relacionarse

[52] https://urldefense.proofpoint.com/v2/url?u=https-3A__www.lesechos.fr_idees-2Ddebats_cercle_cercle-2D165613-2Dlinnovation-2Dlautre-2Darme-2Ddu-2Dbrexit-2D2061519.php&d=DwIFAw&c=jxhwBfk-KSV6FFIot0PGng&r=Fk3CDN4QpXmXZZ7F2MuwcJTW5M0wnTw0gqFJV2no8r8&m=Yd8qNquweowj_8BlDbM5Ljgl43DBuw5ZitB6SZdhk7E&s=UHTdvy5zVo0ee3dA1N5JRiq8X9UDsOY4hU1BgUuAcUc&e.

[53] https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2017/7/personal-data-protection-seminar-2017.

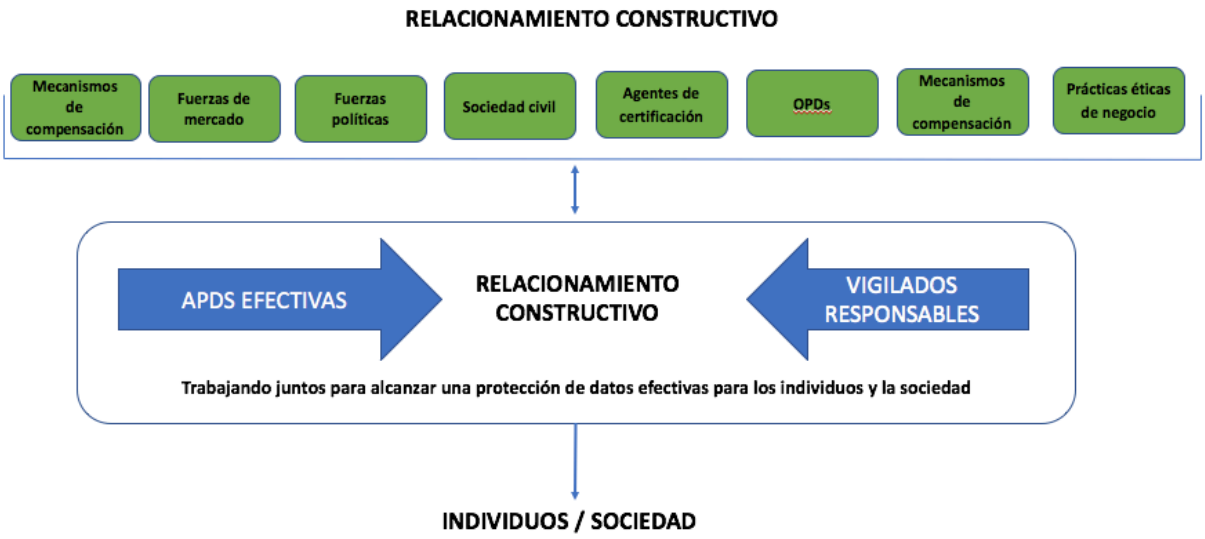
constructivamente con las APDs. Esto significa dar el paso adelante —tanto proactiva como reactivamente—con una aproximación tan franca y abierta como sea posible. Las empresas y las entidades públicas deben ser capaces de explicar y demostrar de la forma más transparente posible, sus procedimientos y soluciones tecnológicas y estar listos para explicar y demostrar sus métodos de negocio. Esto también es una cuestión de *interés propio ilustrado* y es especialmente prometedor en un ambiente donde más y más entidades responsables se enorgullecen de su responsabilidad proactiva. Allí donde se esté desarrollando una propuesta obviamente innovadora o controversial, valioso para identificar de forma anticipada cualquier modificación que asegure la aceptabilidad—cosa que es mucho mejor que las disputas ocurridas después del lanzamiento. En la UE, los mecanismos innovadores del RGPD como la ventanilla única, la autoridad principal, así como la cooperación y los procedimientos de consistencia, deberían promover este diálogo de doble vía, que es más transparente y se basa en la confianza y el respeto mutuos.

"Necesitamos que las autoridades sean independientes, de la misma manera que necesitamos que los jueces y árbitros sean independientes. Sin embargo, la independencia no puede llegar sacrificando la responsabilidad proactiva ni el relacionamiento y las autoridades se deben mantener con la mira puesta en el pulso del mercado mediante la interacción con la industria y los consumidores … De forma sintética, las autoridades deben relacionarse pero no enredarse, distanciarse pero no aislarse"[54].

El taller de CIPL en Dublín también enfatizó que el relacionamiento constructivo se debe extender más allá de la relación directa entre Autoridad y Vigilado. Además de la importancia obvia de interactuar con los individuos que son los beneficiarios de la protección de datos, hay muchos otros jugadores y fuerzas que pueden invocarse para alcanzar los resultados regulatorios deseados. Como ya se mencionó, los OPDs, terceros certificadores y esquemas de resarcimiento pueden usarse para reforzar el rol de Liderazgo de las APDs. Acudir a los medios y a las fuerzas del orden político es vital para comunicar mensajes. La presión de un mercado competitivo, donde las organizaciones le dan un valor enorme a la reputación, también se tiene que entender y aprovechar.

El relacionamiento constructivo puede caracterizarse como operando dentro de un "Marco" que captura las contribuciones de esta rica red de partes interesadas (*stakeholders*). El diagrama del marco que se incluye ilustra el alcance que tienen las APDs para vincularse directamente con esos vigilados, pero también para trabajar con una gama amplia de otras fuerzas y organizaciones.

[54] 'Are regulators the new *Men in Black*?' Cavassini, Naru & Below, en *Risk & Regulation* (LSE, 2016) citando a la OCDE, Being an Independent Regulator.



PREGUNTA PARA DISCUSIÓN

1. **¿Qué actividades y técnicas pueden promover mejor un relacionamiento constructivo en la práctica?**

7. Principios para una Aproximación Basada en Resultados

Una aproximación estratégica para definir prioridades y para tomar decisiones difíciles es esencial para la efectividad de las APDs. Esto se aplica para cada APD individual, pero como la necesidad de coordinación global y consistencia aumenta inexorablemente, también es necesario que se dé la máxima discusión y se alcancen los más amplios consensos sobre la mejor forma de maximizar la efectividad.

Tanto desde la evidencia general sobre vigilancia efectiva descrita en la sección 4, como desde los análisis más específicos de prioridades de protección de datos de la sección 5, es posible conectar los puntos y sugerir un primer borrador para discusión de los Principios de alto nivel que servirían como base para una Aproximación Basada en Resultados. Los principios sugeridos que se ponen de presente abajo están en línea con aproximaciones que ya han sido adoptadas por algunas APDs. Los Principios, sugeridos para discusión en esta etapa, están pensados para ayudar con la definición de prioridades —tanto en términos de

organizar un ranking de funciones entre estas como para definir a qué sectores, actividades u organizaciones se les debería apuntar.

El borrador de los principios está pensado tanto para proveer un Marco para una Aproximación Basada en Resultados, como para aportar a un máximo nivel de consistencia en las estrategias de las APDs. Los principios, entonces, han sido redactados para tener una aplicación amplia para las autoridades de privacidad y protección de datos global y regionalmente. La importancia de trabajar en equipo para asegurar el cumplimiento a través de las fronteras ya se ha mencionado. Pero debe haber una consistencia en la estrategia, así como intercambio de información y agregación de recursos.

Si en su esencia son ampliamente aceptados, se prevé que una versión revisada de los Principios se pueda adoptar y promulgar en cuatro niveles:

- Globalmente, por la Conferencia Internacional de Comisionados de Protección de Datos y Privacidad. Un objetivo razonable sería apuntarle a la 40 Conferencia Internacional, programada para el otoño de 2018.
- A nivel de la UE, por el GT29 y, a su debido tiempo, por el Comité Europeo de Protección de Datos. Idealmente, esto se haría antes de la entrada en vigencia del RGPD en mayo de 2018.
- A nivel de Asia – Pacífico por el foro de Autoridades Asia Pacífico (APPA).
- A nivel operativo, por el Global Privacy Enforcement Network (GPEN) y el APEC Cross-border Privacy Enforcement Arrangement (CPEA)

Principios para una Aproximación Basada en Resultados

- Para poder Vigilar en busca de Resultados en un mundo digital, se requieren Autoridades de Protección de Datos independientes y que sean estratégicas, efectivas, coordinadas y transparentes.

- El objetivo de una APD debe ser producir resultados efectivos en términos de costos, que protejan realmente a los individuos, promuevan usos responsables de la información y faciliten la prosperidad y la innovación

- Las APDs deben tener la protección de los individuos en lo más alto de sus prioridades.

- Cada APD independiente debe ser responsable de informar sobre los resultados que busca alcanzar y las prioridades y aproximaciones que adoptará para alcanzar esos resultados en su labor de vigilancia.

- Las estrategias de todas las APDs deben ser tan coordinadas, consistentes y complementarias como sea posible.

- Cada APD debe adoptar una aproximación basada en riesgos para todas sus actividades, fijando las prioridades en aquellas conductas que generen mayor riesgo a los individuos o a los valores democráticos y sociales.

- Una aproximación basada en el relacionamiento constructivo con énfasis en liderazgo, información, asesorías, diálogo y apoyo será más efectiva que la simple y excesiva dependencia en la disuasión y el castigo.

- El énfasis en la información y la asesoría es especialmente importante en el área de protección de datos, debido a su amplio impacto en tantas organizaciones y a la naturaleza de los requerimientos que, o son imprecisos, o son determinados por el contexto, requiriéndose que haya juicios de valor caso por caso.

- Las relaciones abiertas y constructivas con las organizaciones que tratan datos personales, basadas en un diálogo constructivo y en la cooperación mutua, pero sin caer en responsabilidades difuminadas, mejorarán los resultados generales de cumplimiento legal.

- Las organizaciones vigiladas deben ser evaluadas particularmente con referencia a la buena fe demostrable y a la debida diligencia empleada en sus esfuerzos para cumplir con la ley.

- Las organizaciones que intentan comportarse de manera responsable para "hacer lo correcto" deben tener incentivos para identificarse, por ejemplo mediante la demostración transparente de su responsabilidad proactiva, sus programas de protección de datos y gestión de riesgos, la influencia de sus OPDs y el uso de sellos y programas de certificación, BCRs, CBPR y otros marcos de responsabilidad proactiva (*accountability)*.

- Las sanciones punitivas deben dirigirse principalmente a la actividad que, de manera consciente, deliberada, seriamente negligente, reiterada o particularmente grave, incumpla con la ley.

- Las APDs deben tratar a las organizaciones vigiladas de manera consistente—adoptando aproximaciones similares dentro de ciertos sectores, independientemente del tipo o alcance geográfico de la organización.

- Aunque la necesidad de gestionar quejas individuales puede ser un componente importante para proteger a los individuos, manejar volúmenes muy altos consume muchos recursos y puede impedir alcanzar metas

estratégicas más amplias. Las quejas deben ser gestionadas con criterios estrictos y claros para determinar el alcance de las investigaciones, y también teniendo en cuenta que son un recurso de inteligencia muy valioso.

¿Un protocolo?

Cualquier grupo de Principios está llamado a ser de alto nivel y aspiracional. Puede ser prematuro para considerar cómo dotarlos de más contenido y traer a la vida una Aproximación Basada en Resultados como estándar regulatorio moderno para las APDs. Igualmente, existe un riesgo real de que cualquier intento de articular estándares específicos sea visto como una especie de imposición externa.

No es en absoluto la visión de este artículo proponer requerimientos obligatorios. CIPL tiene claro que las movidas hacia una Aproximación Basada en Resultados en protección de datos deben venir de las propias APDs. Esto no solo teniendo en cuenta su independencia. Dicha aproximación solo está llamada a prosperar si su razonamiento central es acogido por la comunidad de APDs. Nunca puede ser impuesto.

Para ayudar en este proceso, y para juntar las principales ideas descritas en este artículo y estimular futuras discusiones, CIPL ha creado un primer borrador de Protocolo para una Aproximación Basada en Resultados para la Vigilancia en Protección de Datos. El borrador de protocolo forma el Anexo D de este artículo.

Como los principios, cualquier Protocolo para APDs solo puede ser aceptado y adoptado de manera colectiva y voluntaria con consensos sobre el marco básico y el lenguaje. Como una posible vía—especialmente con el contexto del desarrollo del Mecanismo de Consistencia—el CEPD podría desarrollar su propio Protocolo para dotar de vida a los Principios y después promover su adopción por todas las APDs de la UE.

A nivel mundial, (particularmente a través de la red de APPA y/o operativamente a través de GPEN y el CPEA) el mismo Protocolo podría ser adoptado por las APDs o podría tomarse el borrador del Anexo D como el punto de partida para desarrollar algo más a la medida.

PREGUNTAS PARA DISCUSIÓN

1. ¿Los organismos que coordinan a las APDs a nivel global, regional y operacional considerarían adoptar los Principios sugeridos para alcanzar una Aproximación Basada en Resultados?

2. ¿Cómo se pueden mejorar los Principios sugeridos?

8. Posibles problemas

Todas las estrategias involucran decisiones difíciles. Debe reconocerse abiertamente que una Aproximación Basada en Resultados puede traer algunos retos y riesgos. Cualquier ranking de prioridades implica “perdedores” así como “ganadores”. El relacionamiento con las organizaciones vigiladas puede ser contraproducente y generar preocupaciones genuinas—tanto de que las APDs se conviertan en “cautivas” y que algunos vigilados no estén muy contentos con una excesiva relación con la APD sobre sus actividades pasadas, presentes y futuras.

a. Reticencia a relegar funciones

Las APDs mismas se podrían poner nerviosas con la asignación de una menor importancia a cualquier función que esté descrita en términos de un deber legal. Como se puso de presente anteriormente, en la UE muchas de las funciones del RGPD están escritas como “tareas” que la APD debe “llevar a cabo”. En la medida en que el RGPD no provee ningún objetivo estratégico de carácter general para las APDs ni ninguna autoridad explícita para posicionar alguna actividad por encima de otras, las APDs se pueden mostrar renuentes a llevar a cabo ese ranking por sí mismas.

Hay, sin embargo, varias respuestas a estas preocupaciones. No obstante la falta de autoridad explícita, algunas APDs ya adoptan sus propios valores u objetivos de alto nivel. Una aproximación estratégica y transparente es preferible a cambios *ad hoc* e impredecibles, motivados por los eventos del día a día, de una actividad a otra. El que se encuentre en la parte baja del ranking, o bien por una gestión estricta de la demanda, no significa abandonar cualquier función completamente—y esto no es algo que se sugiera aquí. Incluso cuando no hay una discreción explícita, aún habrá campo para ejercer el buen criterio y la proporcionalidad. De manera creciente se ha venido convirtiendo en la norma, por ejemplo para otras autoridades de vigilancia, darle prioridad a las funciones de Liderazgo en la medida que son más efectivas para cambiar los comportamientos que el rol de Oficial de Policía. En efecto, podría ser inapropiado para cualquier autoridad embarcarse en actividades sancionatorias, para imponer multas cuantiosas, por comportamientos que antes no había señalado como inaceptables.

Igualmente, una política general de gestionar de manera estricta las quejas, pero considerar algunas como dignas de mayor atención, es enteramente posible. Por ejemplo, las quejas comúnmente se reciben y se registran como evidencia preliminar de un problema y sin embargo la inmensa mayoría no se pueden someter a investigaciones detalladas. La profundidad de la investigación en esa medida es proporcional a la potencial gravedad de los asuntos involucrados. Esto requiere de procedimientos robustos para que los componentes clave de cada queja puedan ser rápidamente evaluados y (en la mayoría de los casos) los quejosos puedan saber

por qué para solucionar su caso no pueden dedicarse recursos que son por naturaleza escasos ni esfuerzos desproporcionados.

b. Captura del Regulador

Se pueden generar ciertas ansiedades sobre el darle mayor prioridad al relacionamiento con los vigilados. Puede haber algunas preocupaciones de "Captura Regulatoria" si las APDs se vuelven muy cercanas a aquellas organizaciones que vigilan. La Captura Regulatoria se describe como el proceso mediante el cual un sector regulado puede influenciar o manipular a las agencias que supuestamente las controlan. Esto se puede ver como una amenaza tanto a la independencia como a la integridad de las Autoridades.

Sin duda, las autoridades siempre deben gestionar de manera apropiada sus relaciones con sus vigilados, para limitar el riesgo de "Captura Regulatoria". También deben tener cuidado con las presiones, que por ejemplo podrían resultar en una influencia inadecuada en la selección de los objetivos de vigilancia, una excesiva empatía con las necesidades de sus vigilados o sanciones menos estrictas.

Con máxima transparencia y otros mecanismos de salvaguarda, los temores de Captura Regulatoria deberían permanecer como algo meramente teórico. Como sucede en todos los campos, las autoridades independientes deben ser capaces de tener una "relación de adultos" con aquellos que vigilan. Para esto se necesita contacto con el sector vigilado. Una "cultura de integridad" consciente y abierta le ayudará a las APDs a resistir presiones de los sectores vigilados. Las APDs, con sobrados méritos, están orgullosas de su independencia y son lo suficientemente maduras como para saber que independencia también implica imparcialidad –mirar cuidadosamente a ambos lados de cada asunto y considerar todos los hechos. Una cultura corporativa que promueva la integridad y niveles altos de probidad, quizás con algunas separaciones internas de funciones, le permitirá a las APDs tomar las decisiones correctas sobre los niveles apropiados de relacionamiento con el sector vigilado, tanto formal como informal.

c. Resistencia de los vigilados

Puede haber preocupaciones correlativas de la comunidad vigilada de que el excesivo relacionamiento con las autoridades pueda ser problemático. Algunas organizaciones vigiladas pueden preferir mantener una distancia con la APD, quizás por miedo a una sanción derivada de comportamientos pasados, por exposición de sus documentos o prácticas a la APD durante un periodo de consultas o por temor a un veto frente a una innovación planeada. Esto, sin embargo, sería poco probable. Las organizaciones con una cultura de secreto, irónicamente pueden atraer más atención sobre sí, y es mejor estar informado sobre un incumplimiento de manera

previa en vez de descubrirlo, con costos considerables, en una etapa posterior. Igualmente, una APD se arriesga a dañar su propia reputación y estrategia si se empeñara en aplicar sanciones estrictas en respuesta a informaciones que haya conocido en el curso de una relación supuestamente constructiva.

De forma más general, como ya se puso de presente, el relacionamiento está fuertemente conectado con la responsabilidad organizacional y debe ser un proceso de doble vía basado en la confianza mutua. Los vigilados no pueden esperar que las APDs se involucren en una Aproximación Basada en Resultados a menos que también pongan de su parte.

Anexo A – Funciones de las APD bajo el RGPD

En la siguiente tabla se agrupan las principales tareas y poderes asignados a las APDs agrupadas en una de cuatro categorías. La sección 5 de este artículo usa esta categorización en el contexto del establecimiento de prioridades.

TAREA / PODER	ARTÍCULO
LÍDER	
Promover la conciencia pública sobre riesgos reglas, salvaguardas y derechos	57(1)(b)
Promover la concientización de las obligaciones de los responsables / encargados	57(1)(d)
Asesorar al parlamento, gobierno etc.	57(1)(c)
Proveer información a los titulares por solicitud	57(1)(e)
Monitorear la aplicación de la Regulación	57(1)(a)
Monitorear las tecnologías y prácticas comerciales relevantes etc.	57(1)(i)
Asesorar sobre las operaciones de tratamiento que requieran una EIPD	57(1)(l)
Promover y facilitar los códigos de conducta, mecanismos de certificación y sellos y marcas	57(1)(m)-(q)
AUTORIZADOR	
Autorizar los tratamientos de alto riesgo sobre la base de razones de interés público	58(3)(c)
Autorizar las cláusulas contractuales para las transferencias internacionales	58(3)(h)
Autorizar los acuerdos administrativos para hacer transferencias internacionales	58(3)(i)
Autorizar Normas Corporativas Vinculantes (BCR)	58(3)(j)
Aprobar / acreditar códigos, mecanismos de certificación, y sellos y marcas	42, 43, 57, 58 & 64 *passim*
OFICIAL DE POLICIA	
Hacer cumplir la aplicación de la ley	57(1)(a)
Llevar a cabo investigaciones sobre la aplicación del Reglamento	57(1)(h)
Ordenarle al Responsable / Encargado que provea información	58(1)(a) & (e)
Obtener acceso a las instalaciones, los equipos y los medios del responsable / encargado	58(1)(f)
Emitir advertencias y reprimendas	58(2)(a)-(b)
Dar órdenes de cumplimiento	58(2)(c)-(e)
Imponer limitaciones y restricciones al tratamiento	58(2)(f)
Ordenar la rectificación, borrado etc.	58(2)(g)
Imponer multas administrativas	58(2)(i)

Suspender los flujos internacionales de datos	58(2)(j)
GESTOR DE QUEJAS	
Gestionar e investigar quejas	57(1)(f)

Anexo B - Recursos de las APD

El más reciente sondeo comparativo de presupuestos de las APDs se llevó a cabo por la Conferencia Internacional de Comisionados de Protección de Datos y Privacidad (ICDPPC) en 2017[55]. Las respuestas incluyen datos de 87 autoridades de protección de datos de 58 países. De los países que entregaron información sobre recursos financieros, el presupuesto global total de las APDs para 2016 fue de €887,320,351.[56]

La información de recursos financieros está disponible para todos los países miembros de la Unión Europea con excepción de Austria, Croacia y algunos de los Länder alemanes. CIPL ha tomado los datos financieros de ese sondeo para los 26 países de la UE[57] que están incluidos y los comparó contra las cifras poblacionales. Esas cifras muestran un presupuesto total en 2016 de €205,703,574 para una población total ese año de 507,471,970.[58] Esto sugeriría, a lo largo de esos 26 países en conjunto, que el presupuesto por ciudadano fue menor a €0.41. El dato actual probablemente sería un poco mayor si los presupuestos de Austria, Croacia y todos los Länder alemanes hubieran estado disponibles. Las cifras para 2017 sin duda serán más altas—todos los presupuestos de los Estados Miembros para 2016 incrementaron comparativamente con 2015 con excepción de Portugal, Chipre, Letonia y un Länd alemán—pero es dudoso que el presupuesto per cápita sea significativamente más alto.

Es aún más indicativo de las demandas que pesan sobre cada APD establecer el número de organizaciones vigiladas. A diferencia de muchas otras autoridades, las responsabilidades de las APDs no son sectoriales y cubren todos los sectores de la economía. Adicionalmente, la mayoría de las entidades públicas caen dentro de la jurisdicción de las APDs y, por ejemplo, el RGPD impone requerimientos más estrictos con responsabilidades correlativas a las APDs.

[55] Los datos del censo están disponibles por solicitud en la Secretaría de la Conferencia Internacional de Comisionados de Protección de Datos y Privacidad https://icdppc.org/the-conference-and-executive-committee/icdppc-census/.
[56] Muchos países reportaron su presupuesto en moneda local. Estos se convirtieron a euros usando las tasas de cambio disponibles el 27 de julio de 2017.
[57] La cifra para Alemania es menor que los valores actuales toda vez que solo 7 de los 16 Länder suministraron información.
[58] Las cifras de población se tomaron del Banco Mundial el 27 de julio de 2017 http://data.worldbank.org/indicator/SP.POP.TOTL.

Eurostat estima que “en 2014, la economía comercial del EU28 estaba conformada por alrededor de 26 millones de empresas activas”[59]. Esto presuntamente excluye a la mayoría de las entidades públicas. Muy pocas organizaciones están hoy en día exceptuadas de los requerimientos de protección de datos personales. Incluso la más pequeña empresa unipersonal probablemente trata datos personales de sus consumidores y de otros contactos en un teléfono móvil o un computador personal. Esto sugiere que, a lo largo de la UE, las APDs tienen un presupuesto promedio de alrededor de €8 por empresa.

[59] http://ec.europa.UE/eurostat/statistics-explained/index.php/Business_demography_statistics.

Anexo C – Conclusiones básicas de "Law and Corporate Behaviour"

1) **Un sistema regulatorio es más efectivo cuando es consistente y apoya los comportamientos que son vistos de manera amplia como justos, proporcionales y éticos.**

   Las autoridades deberían adoptar los incentivos y acciones correctas que apoyen, y no menoscaben, los esfuerzos de los individuos y las empresas de comportarse correctamente. Por ejemplo, las autoridades deberían adoptar y publicar estrategias de cumplimiento de la ley que reconozcan los esfuerzos de las organizaciones de hacer lo que es correcto.

   Las autoridades deberían ser cuidadosas de no concentrarse mucho en reglas detalladas o prescriptivas ("aproximación de lista de chequeo") que reduce la habilidad de las organizaciones de pensar por sí mismas y disminuye tanto el poder como el ámbito de actuación para comportarse responsablemente. Las autoridades deberían influenciar la propensión de los negocios exitosos de adoptar culturas basadas en los valores en los que todos se encuentran alineados para enfocarse en alcanzar los resultados esperados. Con una cultura de ese tipo se podrá, por ejemplo, aprender de los errores, evitar las culpas, hacer que las cosas se arreglen cuando se hubieran enfocado de manera equivocada, ser receptivo de las quejas y generar ideas para el mejoramiento y la innovación.

2) **Las organizaciones deben ser responsables y poder demostrar, con evidencia, su compromiso con el comportamiento que atraiga la confianza de las autoridades—así como de sus propias directivos y personal, clientes, proveedores, inversionistas y otros *stakeholders*.**

   Una empresa debería ser alentada—y a veces obligada—a adoptar conductas de negocio responsables en todas las actividades que lleve a cabo. Los códigos en aspectos particulares no son suficientes—la aproximación debe ser holística. Tiene que dirigirse desde la cúpula, pero debe existir en todos los grupos sociales dentro de una organización.

   Las autoridades deberían estar buscando evidencias de que una organización funciona con integridad y tiene una aproximación positiva al cumplimiento legal. Las meras aseveraciones de una compañía de que se puede confiar en ella claramente no serán suficientes. La evidencia puede adoptar tantas formas como las estructuras de gobernanza que pongan énfasis en el cumplimiento, la adherencia consistente a estándares de comportamiento, una proporción alta de clientes satisfechos, una aplicación

consistente del cumplimiento legal, sistemas de auditoría y una aproximación transparente a la verificación externa.

3) **El aprendizaje es fundamental y se estimula con un relacionamiento abierto y constructivo entre las autoridades y las organizaciones vigiladas, pero termina siendo disuadido por un énfasis en la "culpa" y/o el castigo.**

   Los sistemas regulatorios donde son críticos el aprendizaje y el mantenimiento de los buenos resultados—tales como la aviación civil, la fármaco-vigilancia y la salud y seguridad en los lugares de trabajo—se aproximan a la "vigilancia" como un marco de comportamiento que ayuda a las personas a tomar las decisiones correctas a través del aprendizaje continuo.

   Un asunto crítico es identificar por qué ha ocurrido un riesgo o un problema, qué factores actuales o potenciales lo generaron y cómo puede reducirse el riesgo de un evento similar. El énfasis está en el monitoreo constante y en aprender de los acontecimientos, para mejorar los resultados y reducir el riesgo.

   Sin embargo, las personas no estarán dispuestas a entregar información de manera voluntaria si temen que esto atraiga críticas o que se les imputen culpas. Así, con salvaguardas adecuadas, es esencial promover una "cultura abierta" de compartir y preguntar, en vez de una cultura de "culpa" o una relación confrontacional con las autoridades. Esta debería ser la norma excepto en los casos de violaciones graves u obvias de la ley.

4) **Los sistemas regulatorios se deben basar en el diálogo y la cooperación mutua que está explícitamente dirigida a maximizar el cumplimiento, la prosperidad y la innovación.**

   El diálogo permanente y la cooperación mutua que es transparente, en vez de una relación confrontacional y distanciada, son consistentes con los sistemas de gestión, cumplimiento y riesgo. Todos estos involucran mecanismos basados en la circulación de información que monitorea el desempeño, identifica los riesgos y hace mejoras.

   Si el objetivo principal es lograr los comportamientos correctos a través del máximo nivel de cumplimiento, esto se logra mejor mediante la combinación de sistemas regulatorios con acuerdos co-regulatorios estructurados y supervisados. Dichas estructuras co-regulatorias se pueden desarrollar de forma que incluyan compromisos frente a comportamientos éticos y de

cumplimiento, así como mecanismos que generen evidencias que apoyen una relación de confianza.

5) Allí donde las organizaciones violen las reglas, se necesita una respuesta proporcional, donde se reserven las sanciones más altas para las conductas deliberadas, reiteradas o manifiestamente dolosas.

Aun cuando hay obviamente muchos "tonos de gris", un régimen regulatorio moderno distingue entre las personas que básicamente están tratando de hacer lo correcto de aquellas que no lo están—en esencia se trata de un asunto de motivaciones. Tener mecanismos de cumplimiento de la ley justos y proporcionados es importante[60]. Si las personas incurren en escenarios de no cumplimiento que es deliberado, doloso o seriamente negligente, la ley se debe hacer cumplir con una respuesta proporcional. Pero en aquellos casos donde la gente ha venido tratando de hacer lo correcto, pero ha sido ignorante acerca de sus responsabilidades, adoptar una respuesta punitiva podría ser visto como injusto y de poca ayuda en la promoción de la voluntad de cumplimiento.

La aproximación moderna a cómo hacer cumplir la ley, descansa sobre la base de la premisa de que "la mayoría de las organizaciones buscan hacer lo correcto la mayoría del tiempo". Esa aproximación contrasta con una aproximación dominante que es represiva, basada en la disuasión o el castigo. La sicología del comportamiento, especialmente en el contexto corporativo, no apoya la idea de que el futuro cumplimiento – o la disuasión del no cumplimiento— se incremente por las amenazas o la imposición de penas altas. Se ha demostrado que la idea de que las personas en el mundo corporativo obedecerán la ley por miedo a que un incidente será castigado, con lo cual es mejorar adecuarse que sufrir, solo es efectiva cuando se percibe un riesgo alto de identificación seguido de la pérdida de la reputación personal o corporativa. El prospecto de una penalidad financiera al negocio no es una motivación fuerte para el cumplimiento legal. Vigilar usando el miedo, en una democracia moderna, es en cualquier caso una política muy poco atractiva.

[60] Ver también RGPD, Artículo 83(2).

Anexo D – Primer borrador de un posible Protocolo

Borrador de Protocolo para una Aproximación Basada en Resultados para la Vigilancia en Protección de Datos

1. **La efectividad de las autoridades de protección de datos se mide fundamentalmente por el grado de protección práctico de los individuos.**

2. **Las Autoridades de Protección de Datos deberían asegurar que haya disponibilidad de información, guías y asesorías claras para ayudarle a sus vigilados a cumplir con sus obligaciones.**

- Las APDs deben dar asesorías y guías que se enfoquen en ayudarle a los vigilados a entender y cumplir con sus obligaciones. Cuando estén dando estas asesorías y guías, se debe considerar su impacto de forma que no se creen cargas innecesarias para la propia APD.

- Las APDs deberían escribir toda información, guía y asesoría en lenguaje sencillo y usar formatos y medios claros, concisos y accesibles que sean apropiados para su audiencia objetivo. Deberían solicitar comentarios, tan pronto como sea posible, sobre las guías que se planea expedir.

- Las APDs deben crear un ambiente en el que sus vigilados tengan confianza en los consejos que reciben y se sientan seguros de pedir dicho consejo sin temor a desatar una acción investigativa.

3. **Las Autoridades de Protección de Datos deben ofrecer canales claros y sencillos para relacionarse con sus vigilados y escuchar sus opiniones.**

- Las APDs deberían establecer mecanismos para relacionarse con sus vigilados permitiéndole a los ciudadanos y a otros ofrecer sus puntos de vista y contribuir al desarrollo de sus políticas y sus estándares de servicio.

- Cuando hagan frente al incumplimiento, las APDs deben explicar de manera clara cuál es el punto o la actividad que no cumple, el consejo que se da al respecto, las acciones requeridas o las decisiones adoptadas y las razones para éstas. Las APDs deberían ofrecer una oportunidad para el diálogo en relación con los consejos, requerimientos o decisiones, con miras a asegurar que están actuando en forma proporcional y consistente.

- Este parágrafo no aplica cuando las APD puedan demostrar que se requiere una acción cautelar o sancionatoria inmediata para prevenir o responder a un incidente serio o donde aplicar dicha oportunidad podría resultar en un menoscabo del propósito de la acción de cumplimiento propuesta.

- Las APDs deben asegurar que haya una forma imparcial y claramente

explicada para apelar las decisiones sancionatorias.

- Las APDs deberían pedir, recibir y aplicar la retroalimentación regularmente, por ejemplo a través de encuestas de satisfacción a sus vigilados.

4. **Las Autoridades de Protección de Datos deberían adelantar sus actividades de manera que apoyen a aquellos que buscan cumplir con las normas.**

- Las APDs deben escoger aproximaciones proporcionales para aquellos que vigilan, basándose en factores relevantes que incluyen, por ejemplo, el tamaño de las organizaciones y su capacidad y los volúmenes y naturaleza de los datos personales que tratan.

- Cuando se diseñan y se revisan las políticas, procedimientos operativos y prácticas, las APDs deberían considerar cómo podrían apoyar o permitir la innovación y el crecimiento económico para los negocios que sí cumplen, por ejemplo teniendo en cuenta cómo pueden:

  - alentar y promover el cumplimiento;

  - mejorar la confianza en el cumplimiento para sus vigilados ofreciendo para ello el mayor grado de certeza;

  - entender y minimizar los impactos económicos negativos de sus actividades de vigilancia; y

  - minimizar los costos de cumplimiento para sus vigilados.

5. **Las Autoridades de Protección de Datos deberían basar sus actividades en el riesgo.**

- Las APDs deberían adoptar una aproximación basada en evidencias para determinar los riesgos prioritarios en sus áreas de responsabilidad, y deberían destinar recursos donde sean más efectivos para atender dichos riesgos prioritarios.

- Las APDs deberían tener en consideración los riesgos en todas las etapas de sus procesos de toma de decisiones, incluyendo escoger el tipo más apropiado de intervención o la forma de trabajar con sus vigilados. La valoración de riesgos también se debería usar para hacer revisiones de cumplimiento y para decidir sobre las investigaciones que se van a adelantar.

- Las APDs, cuando hacen la valoración de riesgos, deberían reconocer la responsabilidad proactiva y el record de cumplimiento de sus vigilados (por ejemplo mediante el uso de aproximaciones de reconocimientos por méritos) y deberían tener en cuenta toda la información disponible y relevante sobre cumplimiento incluyendo la evidencia de verificación externa relevante.

- Las APDs deberían revisar la efectividad de sus actividades de vigilancia

para que generen los resultados deseados y además hacer los ajustes que sean necesarios de conformidad con esa premisa.

6. **Las Autoridades de Protección de Datos deberían asegurar que su aproximación a las actividades de vigilancia sea transparente y consistente, y bien coordinada con las aproximaciones de otras autoridades.**

- Las APDs deberían publicar sus estrategias, planes anuales, estándares objetivos, etc. para que sus vigilados sepan qué esperar de ellas. Esto debería incluir, por ejemplo, información clara sobre:

  - cómo se comunican con sus vigilados y cómo pueden ser contactados;

  - su aproximación a dar información, guías o asesorías;

  - su aproximación a la revisión del cumplimiento legal, incluyendo detalles sobre el marco de evaluación de riesgo usado para escoger dichas revisiones; y

  - la política de investigaciones y acciones de cumplimiento, explicando cómo responden frente a la falta de cumplimiento.

- En una sociedad digital donde los datos no reconocen las fronteras nacionales, las APDs deberían maximizar la efectividad, consistencia y eficiencia a través de una coordinación cercana y una cooperación con sus pares en otras jurisdicciones.

Bibliografía

Este artículo de discusión se ha nutrido de varias fuentes. Las siguientes publicaciones son particularmente útiles.

Responsive Regulation – Ian Ayres y John Braithwaite, OUP, 1995.

A Reader on Regulation – Baldwin, Scott & Hood, OUP, 1998.

The Regulatory Craft – Malcolm K. Sparrow, The Brookings Institution, 2000.

The Governance of Privacy – Colin Bennett y Charles Raab, MIT Press, 2006.

Implementing Hampton: From Enforcement to Compliance – UK Better Regulation Executive, 2006.

Really Responsive Regulation – Baldwin & Black – LSE, 2007.

Risk and Regulatory Policy - Improving the Governance of Risk – OCDE, 2010.

The Governance of Regulators - Best Practice Principles for Regulatory Policy – OCDE, 2014.

Law and Corporate Behaviour - Integrating theories of regulation, enforcement, compliance and ethics – Christopher Hodges, Hart Publishing, 2015.

The European Union as Guardian of Internet Privacy – Hielke Hijmans, Springer, 2016.

Regulatory Theory - Foundations and Applications – Peter Drahos, Australian National University, 2017.