Sistematización Comentarios Consulta Ciudadana y Recepción de Ideas Protección de Datos Personales

Consejo para la Transparencia

I. Presentación

Entre el lunes 22 de junio y el domingo 19 de julio de 2020, se realizó el Proceso de Consulta Pública sobre Protección de Datos Personales (PDP) en la plataforma ParticipaTransparente[1] del Consejo para la Transparencia (CPLT). Esta plataforma pretende ser un espacio virtual para la instalación de diversos mecanismos establecidos en la Política de Participación del CPLT y contribuir al objetivo estratégico de "*Promover y difundir el principio de transparencia, el derecho de acceso a la información pública y la protección de datos personales como herramientas de la rendición de cuentas de autoridades y de control social, así como para favorecer el ejercicio de otros derechos*".

La Dirección de Promoción, Formación y Vinculación del CPLT, cuenta con un Programa de Redes y Participación que establece, dentro de sus componentes de vinculación con la ciudadanía y Organizaciones de la Sociedad Civil, el establecimiento de mecanismos e instancias de participación presencial o virtual. En esta línea, contribuyendo a la incorporación de la sociedad civil en ámbitos de acción del Consejo, se propuso iniciar un Proceso de Consulta Ciudadana, en modalidad piloto, en materia de Protección de Datos Personales, para lo cual se invitó a *stakeholders* relevantes en la materia vinculados a PDP en las siguientes esferas:

- Académica: Universidades o Centro de Investigación asociadas al ámbito legal (PDP, Derechos Fundamentales).
- Científica: Instituciones públicas o privadas vinculadas al manejo de datos con propósitos científicos (Big Data, datos abiertos, etc.).
- Organizaciones de la Sociedad Civil (OSC): con trabajo en Protección de Datos y Datos Abiertos.
- Think Tanks o Centros de Pensamiento: con líneas de investigación asociadas a datos abiertos y PDP.
- Ámbito privado: eventuales sujetos obligados por la nueva normativa en Protección de Datos Personales, tales como Asociaciones de Retail, Banca, Inmobiliarias, Desarrolladores Tecnológicos, cadenas de farmacias, etc.

La invitación se envió entre el 29 de junio hasta la semana de cierre, del 13 de julio, desde el correo institucional vinculacion@cplt.cl y/o desde el correo del Director de Promoción, Formación y Vinculación del CPLT.

En la página web se podía participar a través de dos formas: respondiendo la consulta a través de un formulario y/o proponiendo ideas en la plataforma. Para orientar los aportes, se sugirió dar respuesta a las siguientes preguntas:

- Debilidades del Estado en tratamiento de Datos Personales: ¿Qué brechas identifican en los Organismos del Estado para abordar un tratamiento adecuado de los Datos Personales?

[1] https://participatransparente.cl/es-CL/projects/consulta-ciudadana-proteccion-de-datos-personales/process

- Riesgos para la convivencia social asociados al tratamiento de Datos Personales: ¿Qué riesgos en materia de discriminación hacia las personas y/o grupos sociales conlleva un tratamiento deficiente de Datos Personales? ¿Cómo debieran ser abordados estos riesgos?

- Rol del Consejo para la Transparencia en PDP – Prioridades y desafíos de gestión. ¿Cuál debiera ser el Rol del CPLT como garante de la PDP? ¿Cuáles debieran ser sus líneas de acción prioritarias y públicos objetivos?

Se recibieron 10 respuestas a la consulta y 1 idea (en Anexos 1 y 2), las que se desagregaron por comentarios según temas que abordaban, de la siguiente forma: 1. Diagnóstico, en el que se abordan a) las brechas para abordar un tratamiento adecuado de los Datos Personales, b) los riesgos en materia de discriminación hacia las personas y/o grupos sociales de un tratamiento deficiente de datos personales y c) las formas de abordar esos riesgos, y 2. el Rol del Consejo para la Transparencia en protección de datos personales, donde se abordan a) las brechas que debe resolver el CPLT y b) cuál debiera ser su rol como órgano garante.

Tabla 1. Comentarios por tema

Temas	N° Comentarios
1. Diagnóstico	
a) Brechas	14
b) Riesgos	10
c) Formas de abordar los riesgos	4
2. Rol del CPLT en PDP	
a) Brechas CPLT	4
b) Rol del órgano garante	13
Total comentarios	**45**

II. Resumen

Las personas que participaron en la Consulta Ciudadana y Recepción de Ideas coinciden en que estamos en una situación de necesidad de una verdadera protección de datos personales (PDP), porque la actual ley es ambigua en la regulación del tratamiento de datos por parte de los órganos del Estado, existe desconocimiento de la normativa PDP y hay una falta de compromiso con la protección de datos personales en los funcionarios públicos. Además, se considera que no existen las condiciones para la circulación de datos personales con estándares adecuados de protección, lo que se evidencia en que no hay medidas de seguridad apropiadas, de ello se desprende que hace falta un órgano garante de PDP. Además, se considera que desde el Consejo tiende a haber un desbalance entre PDP y Acceso a la Información, priorizándose el segundo, en los casos en que se ponderan ambos derechos.

La falta de regulación en PDP provocaría, para los participantes de la Consulta, una serie de riesgos de discriminación hacia las personas, principalmente un tratamiento deficiente de Datos Personales, incluyendo datos desactualizados, lo que conlleva una posible estigmatización, discriminación, vulneración de derechos y exclusión social, lo que se evidencia con la actual recolección desproporcionada de información personal sin consentimiento, además, en la comunicación de datos personales entre instituciones, existe el riesgo de hacerlo sin establecer una finalidad clara. Adicionalmente, se percibe que la falta de sanciones a la vulneración del derecho de protección de datos personales aumenta la desconfianza.

Si bien se identifican riesgos y brechas, no está tan claro cómo debieran ser abordados, al respecto se propone realizar un benchmarking de políticas públicas de protección de datos personales de países avanzados en la materia, lo que contribuiría a adoptar las mejores prácticas identificadas. También se menciona la necesidad de que el CPLT aplique correctamente la ley de protección de datos existente -se considera que hasta ahora no lo ha hecho-, y para ello, en su estructura orgánica/decisoria debiera haber Consejeros que adhieran a los principios y normas de PDP. También se propone realizar un análisis de impacto de medidas de protección de datos, para determinar cuáles cumplen el objetivo de la ley y que los sujetos obligados puedan implementar las medidas de seguridad realmente efectivas.

En la mayoría de las respuestas recibidas, a excepción de una, se percibe al Consejo como el organismo que estará a cargo de la PDP, sin embargo, se mencionan cambios que debiera realizar para ello: la necesidad de un cambio cultural hacia la protección de datos personales -pues se considera que prioriza la entrega de información-, además, se plantea que debiera hacer cambios en su gobierno corporativo, que apunten a lograr equilibrio y rendición de cuentas, también se señala que para lograr instalar el derecho de protección de datos personales como un derecho humano en la sociedad, es necesario que se vincule con la sociedad civil, resguarde su autonomía, mejore su capacidad técnica, cuente con recursos humanos y desarrolle una *expertise* que le permita evaluar el impacto de las medidas que se tomen para la protección de datos personales.

Respecto de su rol como órgano garante de PDP, se considera que debiera tener un rol de promotor del derecho de protección de datos personales, con énfasis en derechos sociales, un rol propositivo respecto a acciones de protección de datos personales en la política pública, especialmente como órgano garante, y la necesidad de coordinar a los diferentes actores para alinear prioridades y objetivos. Así, debiera cumplir un rol orientador de la política pública, estableciendo pautas y parámetros claros para PDP por parte de los sujetos obligados, que permitan prevenir la vulneración del derecho. Se considera que ello, además, contribuiría a disminuir la desconfianza en las instituciones públicas. Como órgano garante, se establece que debe disuadir de la vulneración de la norma, para lo cual debe especializarse en la materia, de manera de fortalecerse en este nuevo rol. De esta forma, se considera relevante el rol fiscalizador, sobre todo en la puesta en marcha de la normativa, cuando a los sujetos obligados, especialmente del sector privado, les pueda costar más cumplir con las exigencias, o presenten resistencias, y ante esto, debiera sancionar los incumplimientos.

III. Resultados

1. Diagnóstico

a) Brechas (14 comentarios)

Se consultó sobre las brechas, específicamente: ¿Qué brechas identifican en los Organismos del Estado para abordar un tratamiento adecuado de los Datos Personales?

Desconocimiento de normativa PDP y falta de compromiso con la protección de datos personales en los órganos del Estado (4 comentarios)

Se plantea como brecha en los organismos del Estado, el desconocimiento sobre qué se entiende por datos personales, la normativa, su aplicación en el tratamiento de los datos personales y las responsabilidades que ello tiene para las instituciones. Por ende, también se verifica una falta de capacitación al respecto entre los funcionarios.

Al problema del desconocimiento, se suma, la falta de compromiso con la protección de datos personales de directivos o jefes de servicio de los órganos del Estado en general.

"Existe muy poco conocimiento de la importancia que tiene el tratamiento de los datos personales".

"Educación y capacitación respecto de que se debe entender por Datos personales, marco de responsabilidades que esto implica (…) capacitación en lenguaje claro del derecho constitucional".

"Falta de capacitación, no hay conocimiento de la normativa, de cómo aplicarla y como llevarla a la práctica más allá de generar documentos (…) Falta de compromiso con la protección de datos desde la más alta dirección, incluso en organismos donde es crítico".

"Hay mucho desconocimiento de la ley por parte de funcionarios también".

No hay condiciones para la circulación de datos personales PDP (2 comentarios)

Se considera que los organismos públicos no cuentan con las condiciones necesarias para la circulación lícita de los datos personales entre instituciones. Además, es necesario que al interior de las instituciones exista un nexo, comunicación, entre las diferentes áreas para lograrlo.

"No existe en el Estado una libre circulación de datos en las condiciones debidas. Los organismos públicos con competencias para hacer tratamiento de datos son incapaces de generar beneficios públicos porque no lograr crear "las condiciones debidas" para su circulación lícita. El tratamiento nace y muere en ellos de manera aislada".

"Falta construir puentes entre las áreas de negocio, tics y jurídicas".

No hay medidas de seguridad (3 comentarios)

Se considera un problema que no sea obligatorio para los organismos del Estado el contar con políticas de privacidad, encargados o delegados de protección de datos personales, ni medidas de seguridad para resguardar los datos personales que manejan.

"Ausencia de obligación de políticas de privacidad en los tratamientos de datos personales. No hay delegados de protección de datos personales en los órganos del Estado".

"Una primera brecha importante está constituida por la carencia de medidas sistemáticas de seguridad para resguardar la integridad, disponibilidad y confidencialidad de la información personal en poder del Estado, y la necesidad de implementarlas".

"Hay trámites que no indican confidencialidad de los datos, o bien que existen rumores sobre la no confidencialidad. Por ejemplo, denuncias ante la Dirección del Trabajo, es conocido que mucha gente no hace porque se dice que el empleador accede a esos datos".

Falta un órgano garante de PDP (3 comentarios)

Se considera una brecha que no exista un órgano garante -independiente, técnico y con atribuciones-, que entregue estándares, lo que posibilita que el cumplimiento de la protección de datos personales varíe entre los diferentes órganos.

"No existe institucionalidad o esta es difusa y desconocida por la comunidad".

"No existe una entidad que vele por su cumplimiento, fiscalizando e impartiendo estándares, por lo que varía entre distintos organismos".

"Los riesgos en relación a los derechos de las personas por el tratamiento abusivo de los datos personales se morigerarían si existiera una autoridad independiente, técnica y con atribuciones suficientes como para comprender las lógicas del tratamiento de datos personales".

Actual la ley es ambigua en la regulación del tratamiento de DP por parte de los órganos (1 comentario)

Se considera que en la actual ley de Protección de datos personales (19.628) el artículo que habilita a los órganos de la administración del Estado a tratar datos personales **es ambiguo y amplio**, en cuanto permite que lo hagan sin consentimiento del titular cuando sea en relación con materias de su competencia, por tanto, queda a criterio del organismo, sin entregar parámetros específicos para determinar si puede hacerlo o no.

"Por regla general, el tratamiento de datos personales por parte de organismos públicos tiene como fundamento el artículo 20 de la Ley Nº 19.628, y no el consentimiento del titular. Sin embargo, la utilización en la ley de la expresión "respecto de las materias de su competencia" resulta ambigua, y no entrega parámetros para evaluar de forma más precisa si un organismo público puede o no puede ampararse en esta causal de habilitación".

Desbalance entre PDP y DAI en el CPLT (1 comentario)

Otro problema es que actualmente, en la resolución de casos del CPLT, se pondera entre el derecho de protección de datos personales y el derecho de acceso a información pública, privilegiando el cumplimiento de la entrega de información. Al respecto se señala que, aunque los órganos públicos comprenden los riesgos de la entrega de información personal, dado que no cuentan con competencias específicas en la materia, no logran exponer adecuadamente sus argumentos ante el Consejo y se determina la entrega.

"Una de las principales brechas emana del error de base de la comprensión de la protección de datos como una excepción a la transparencia en vez de entender que se trata de un derecho autónomo. Este error lleva a que se ponga en balance estos dos derechos haciendo primar uno respecto del otro (normalmente la transparencia) con una escasa comprensión de los derechos que se ven vulnerados o se ponen en riesgo por la divulgación de la información. (…) La información que consta en el Registro de Nic Chile se transparentó por resolución del Consejo. Esa información permite atacar sitios web (contiene la información de la máquina en que están alojados) extorsionar a sus dueños (secuestrando sus sitios), estafar a terceros (suplantar sitios web), entre otros delitos informáticos. Sin embargo, la

Universidad de Chile no logró explicar esta situación ante el Consejo ni este comprender las magnitudes del problema. Otro caso ejemplar en su momento fue la entrega de la base de datos de SERVEL, en que constan datos sensibles de las personas".

b) Riesgos (10 comentarios)

Se consultó sobre los riesgos para la convivencia social asociados al tratamiento de Datos Personales, específicamente: ¿Qué riesgos en materia de discriminación hacia las personas y/o grupos sociales conlleva un tratamiento deficiente de Datos Personales? ¿Cómo debieran ser abordados estos riesgos?

Tratamiento de datos desactualizados (1 comentario)

Dado que no hay condiciones para la circulación de datos personales entre los organismos públicos, se considera un riesgo el tratamiento de datos caducos.

"El riesgo más evidente es el de tratamiento de datos caducos o desactualizados".

Estigmatización y discriminación a grupos vulnerables (4 comentarios)

Dado que la ausencia de políticas de privacidad en el tratamiento de datos personales se considera una brecha, se piensa que ello generaría un riesgo hacia las personas respecto de una posible estigmatización, violencia y discriminación, percibiéndose esta posibilidad, especialmente, en el tratamiento intrusivo de datos personales de grupos vulnerables.

"El Estado recoge datos especialmente de personas pertenecientes a grupos vulnerables o grupos desaventajados y los somete a tratamientos altamente intrusivos. Ejemplo: reconocimiento biométrico en raciones de comida JUNAEB".

"Estigmatización a grupos vulnerables, violencia en redes sociales, publicación masiva, etc. Estos actos pueden ser realizados por personas, como por instituciones (conocidos casos de amenazas en redes por parte de fuerzas de seguridad)".

"Riesgos de discriminación en cuanto al acceso al empleo, a la educación y a la salud, fundamentalmente".

"Sumados a otras prácticas de recolección extensiva y de perfilamiento, bajo dudosas condiciones de consentimiento informado, convierten al tratamiento de datos personales en un mecanismo cada vez más avanzado para la exclusión social. (…) Otro riesgo está vinculado a la recolección de datos conductuales, historial de compras u otros datos relativos a los hábitos de las personas, junto con la creación de datos inferidos, con la finalidad de perfilar a los usuarios. A medida que el comercio detallista, el sector financiero y otros sectores económicos echan mano a estos mecanismos para realizar publicidad dirigida o determinar el precio de primas de seguros, aumenta el riesgo que este perfilamiento o encasillamiento sea utilizado de forma arbitraria o discriminatoria".

Vulneración de derechos (2 comentarios)

Dado que se considera que existe un desbalance entre PDP y DAI, inclinándose la balanza hacia la entrega de datos personales, más que a su resguardo, se percibe que existe un riesgo de vulneración de los derechos de las personas asociado a ello.

"Es una visión sesgada pensar que el tratamiento de datos personales abusivo se reduce a la discriminación de las personas. El riesgo alcanza a todos y cada uno de los derechos de las personas. Baste el ejemplo a que se aludió antes, en que el derecho de propiedad, la seguridad personal, la seguridad nacional, etc., se puede ver afectada por la entrega indiscriminada de la base de datos de Nic Chile".

"Los mayores riesgos que se aprecian son las denominadas funas que quedan en la impunidad al relativizarse lo privado y personal en beneficio de la publificación de todo y asignarle a la publicidad un valor moral y mayor protección jurídica que a la vida privada. Hay un desbalance entre lo público y lo privado".

Recolección desproporcionada de información personal sin consentimiento (1 comentario)

Dado que no hay medidas de seguridad, es decir, que no es obligatorio para los organismos del Estado el contar con políticas de privacidad, encargados o delegados de protección de datos personales, ni medidas de seguridad para resguardar los datos que manejan, se perciben como riesgo la recolección desproporcionada de información personal sin el consentimiento del titular.

"En primer lugar, constituye una forma de "tratamiento deficiente" la que implica una recolección desproporcionada de información personal, incluida la no relacionada con el giro de quien la solicita ni con la necesidad de identificar a las personas (como en la exclusión por nacionalidad o lugar de residencia). Esto ocurre en un primer nivel con la solicitud de información vinculada a la identificación frente al Estado, y luego con la recolección de información biométrica. (…) En segundo lugar, la convivencia social ya se ha visto afectada históricamente mediante las prácticas de perfilamiento a partir de puntajes de sistema de riesgo crediticio en mercados o para operaciones no directamente relacionadas. El ejemplo histórico de la exclusión por "estar en DICOM" se mantiene en la medida en que no se ilegaliza la exigencia a las personas de exhibir ese puntaje (cuando no puede ser obtenido por la posible contraparte en el otorgamiento de un servicio)".

Comunicación de datos personales entre instituciones, sin el establecimiento de una finalidad clara (1 comentario)

Dado que se considera que la actual ley es ambigua para el tratamiento de datos personales por parte de los órganos del Estado, se percibe en ello un riesgo de comunicación de datos personales entre instituciones, sin el establecimiento de una finalidad clara para su tratamiento y sin garantías de calidad o protección de la información.

"Existe un importante vacío normativo en torno a los requisitos, finalidades y condiciones bajo las cuales una entidad pública puede comunicar datos personales con otros órganos del Estado. Esto conlleva un intercambio no regulado adecuadamente, aumentando el riesgo para los titulares de los datos. En general, se ha utilizado la figura de los convenios de colaboración para realizar estos intercambios, lo que no suelen cumplir con establecer una finalidad clara para el tratamiento de los datos, verificar que el organismo receptor esté habilitado expresamente por ley para procesarlos, y establecer medidas de seguridad y eliminación segura de estos datos, además del cumplimiento continuo de las obligaciones de seguridad. Como consecuencia, y sumado a los puntos anteriores, existe un riesgo alto de tratamiento de datos personales por órganos públicos, no autorizado por ley ni por los titulares, con comunicación entre distintos órganos bajo condiciones de dudosa legalidad, sin fiscalización ni garantías de protección, y sin garantías de calidad ni de eliminación oportuna".

Falta de sanciones aumenta desconfianza (1 comentario)

Otro riesgo derivado de la ausencia de políticas de tratamiento de datos personales es que la falta de sanciones contribuye a aumentar la desconfianza hacia las instituciones públicas.

"Otro riesgo importante es el acceso indebido y la falta de sanciones asociadas al acceso ilegal. Si esta circunstancia no se sanciona queda en la atmósfera la sensación que no existe igualdad ante la ley y se incrementa la percepción de corrupción".

c) Formas de abordar riesgos (4 comentarios)

Realizar un benchmarking de políticas PDP (1 comentario)

Dado que podría haber estigmatización y discriminación a grupos vulnerables, se propone realizar un benchmarking de políticas de protección de datos personales en países avanzados en esta materia para aplicar en Chile las buenas prácticas levantadas.

"Creo que un buen benchmarking con políticas asociadas en países avanzados en esta materia sería positivo. Que se apliquen en Chile las buenas prácticas levantadas a nivel global. Aplicar con énfasis en el caso chileno: alta desconfianza en instituciones públicas y privadas".

El CPLT debiera aplicar correctamente la ley y para ello en su composición debiera haber consejeros que adhieran a los principios y normas de PDP (1 comentario)

Dado que se considera que hay un desbalance entre PDP y DAI, priorizándose la entrega de información, y el riesgo de vulneración de derechos que ello implica, se propone al CPLT que aplique correctamente la ley actual de PDP y para ello se piensa que en su composición debiera haber consejeros que adhieran a los principios y normas de PDP y/o capacitarlos en estos temas.

"En primer lugar, aun sin ley adecuatoria, el Consejo debiera dar una aplicación correcta a la atribución de "velar" por la correcta aplicación de la ley 19.628. Si bien a la fecha han realizado algunos esfuerzos, en sus resoluciones no se aprecia que se haya comprendido el alcance de este derecho ni los riesgos que entraña para la persona la circulación indiscriminada de datos a partir de la entrega incausada de datos que constan en poder de la administración. Esto podría lograrse haciendo educación al interior del consejo (a los consejeros) y a los organismos públicos en la comprensión que deben traspasar al Consejo para que éste pueda resolver correctamente los asuntos en que hay datos personales comprometidos. Generar espacios de reflexión al interior del consejo. En su composición, debiera haber consejeros que adhieran a los principios y normas de protección de datos, que sean capaces de entender los aspectos técnicos del tratamiento de datos".

Implementar medidas de seguridad y hacer un análisis de impacto de medidas (2 comentarios)

Ya que se aprecia que un riesgo es la recolección desproporcionada de información personal y otro la exclusión social, se plantean dos formas de abordarlos: primero, establecer medidas de seguridad, en específico, se menciona la necesidad de incorporar la privacidad en el diseño de herramientas o plataformas tecnológicas, y, en segundo lugar, realizar un análisis de impacto respecto de la protección de datos personales que se logra con estas medidas.

"Estas medidas de seguridad pueden corresponder a mejoras en el diseño de las plataformas digitales y su administración (permisos, privilegios de usuarios), como también de medidas técnicas cuyo objetivo es impedir la filtración, robo, destrucción o mala utilización de la información. En este sentido, los organismos públicos deberán invertir recursos técnicos y humanos para implementar las obligaciones de privacidad por diseño y de seguridad, como las contenidas en el proyecto de ley de datos personales hoy en el Congreso. Estas reglas de seguridad deben también ser aplicadas respecto de las bases de datos hoy existentes, auditando sus contenidos y sus condiciones actuales de seguridad. A ello se suma la necesidad de iniciar evaluaciones de impacto en protección de datos respecto de cualquier iniciativa futura en entidades estatales.".

"Creo que estos riesgos se abordan más allá de la normativa misma. Siempre es útil un análisis de impacto previo para determinar por ejemplo, aspectos relacionados con la calidad de dato o la seguridad que pudieran generar discriminaciones u otras consecuencias indeseables en las personas. Los riesgos deben evaluarse antes del tratamiento y no solo considerar la normativa de privacidad sino aspectos éticos que hoy también son relevantes".

2. Rol del CPLT en la Protección de Datos Personales

Al consultar sobre el rol del Consejo para la Transparencia en la protección de datos personales, de las 10 respuestas recibidas: 1 está en desacuerdo con que sea el CPLT el órgano garante de protección de datos personales.

"No estoy de acuerdo con que desarrolle esta función. En el evento que asuma esas atribuciones y suponiendo que (…)".

1 está de acuerdo explícitamente con que sea el CPLT el órgano garante.

"Ya sea dándole la competencia al Consejo (mi primera opción) u a otra entidad autónoma (…)".

1 aborda el rol del CPLT como órgano garante de manera eventual, pero dándolo prácticamente por hecho.

"El principal rol de CPLT, de transformarse en autoridad pública de control de datos personales, será (…) Respeto a las acciones prioritarias del CPLT cuando se transforme en el órgano encargado (…)".

a) Brechas del CPLT para llegar a ser el órgano garante PDP (4 comentarios)

Cambio cultural hacia la PDP (1 comentario)

Dado el actual rol que tiene el CPLT como órgano garante del derecho de acceso a información pública y la percepción respecto a que, en la ponderación entre PDP y DAI, el Consejo prioriza la entrega de información, se señala que la institución debe avanzar hacia un cambio cultural que instale la cultura de la protección de datos en la organización.

"Como desafíos de gestión al futuro es prioritario instalar culturalmente la protección de datos en la organización. El Consejo es un órgano de transparencia y ya sabemos que la PDP no es la otra cara. Es mucho más amplia y desafiante pues involucra al sector privado".

Cambios en su gobierno corporativo (1 comentario)

La persona que está de acuerdo con que el CPLT sea el órgano garante, plantea que debiera avanzar con cambios en su gobierno corporativo, aunque no se especifica qué cambios en detalle, se apunta a lograr equilibrios y rendición de cuentas.

"Hoy el Consejo tiene una mínima potestad al respecto, pero circunscrita al sector público, sin embargo sin facultades ni muchas capacidades para realmente ejercer dicho rol. (…) Si es el Consejo, es necesario avanzar en ciertas materias en su gobierno corporativo así como también en ciertos equilibrios y rendición de cuentas".

Vincularse con la sociedad civil y resguardar su autonomía (1 comentario)

También se señala que, para lograr instalar el derecho de protección de datos personales como un derecho humano en la sociedad, es necesario que se vincule con la sociedad civil y resguarde su autonomía.

"Para que (sea) el CPLT se requiere un estrecho vínculo con la sociedad civil y el resguardo riguroso de su autonomía".

Desarrollar capacidades internamente (1 comentario)

Se plantea la necesidad de que desarrolle capacidades en materia de PDP para cumplir con las atribuciones jurídicas que tendría, para ello debiera mejorar su capacidad técnica, contar con recursos humanos y se menciona, como ejemplo de la especificidad que se debiera desarrollar en esta expertise, la

necesidad de realizar evaluaciones de impacto respecto de protección de datos personales de acuerdo con la normativa europea.

"Existe un desafío significativo y prioritario en el desarrollo de capacidades para el ejercicio de las labores propias de una autoridad de control (…) Es necesario que una futura autoridad pública de control cuente con suficientes atribuciones jurídicas, capacidad técnica y recursos humanos para llevar a cabo una fiscalización efectiva de estos mecanismos de recolección y análisis de datos. Una alternativa es que los responsables de bases de datos tengan la obligación de reportar a la autoridad de control cuáles fueron las medidas que tomaron para evitar que sus algoritmos vulneren bienes jurídicos que como sociedad consideramos relevantes, como la igualdad en dignidad y derechos. Las evaluaciones de impacto de protección de datos en los términos del RGPD europeo es un mecanismo que sirve a parte de estos fines".

b) Rol del CPLT como órgano garante PDP (13 comentarios)

Se consultó por el rol del Consejo para la Transparencia en PDP, sus prioridades y desafíos de gestión ¿Cuál debiera ser el Rol del CPLT como garante de la PDP? ¿Cuáles debieran ser sus líneas de acción prioritarias y públicos objetivos?

Promotor del derecho (4 comentarios)

Se considera que debiera tener un rol de promotor del derecho de protección de datos personales, con énfasis en derechos sociales, realizando capacitación y difusión del derecho a la ciudadanía.

"Promotor del derecho, auditoría y fiscalización, regulador. Líneas prioritarias: Salud, educación y beneficios sociales".

"El CPLT podría dirigir sus programas de capacitación al público o usuario. *Desarrollo de programas de difusión por etapas (planificación estratégica con indicadores y verificadores claros) socialización de resultados"*.

"Sus líneas de acción al comienzo debieran ser difusión y su público objetivo debiera ser el ciudadano, sin perjuicio de las guías y todo el material de apoyo que debería ser capaz de generar, ojalá actuando de manera proactiva y no reactiva".

"En cuanto al ejercicio de los derechos civiles y políticos, el primer paso es una campaña de educación para que la ciudadanía comprenda que el tratamiento de los datos personales tiene implicancias sociales, políticas y de derechos humanos (…) y una campaña nacional respecto del tema. Aún hay muy poca cultura respecto de que la PDP es un asunto de derechos humanos".

Coordinador de la política pública de PDP (5 comentarios y 1 idea)

Se plantea que es importante un rol propositivo respecto a acciones de protección de datos personales en la política pública, especialmente como órgano garante, y la necesidad de coordinación de los diferentes actores para involucrarlos en alinear prioridades y objetivos.

"Hoy en mi opinión el rol de Consejo ha sido relevante pero a la vez tímido. Se ve comunicacionalmente mucho, pero en la práctica podría hacer mucho más con el "velar por" (…) Hoy el Consejo reacciona en los medios cuando ve injusticias, pero no se ve una política de acción y propositiva que podría explotar aún más".

"Se requerirá un involucramiento significativo con entidades estatales en el ámbito de la ciberseguridad a fines de alinear prioridades y objetivos. Finalmente, se deberá expandir el trabajo de involucramiento regular de las múltiples partes interesadas en la protección de datos personales, para la formación de políticas de la autoridad hacia el futuro y su evaluación".

Así mismo, se plantea que debiera cumplir un rol orientador de la política pública, estableciendo pautas y parámetros claros para la protección de datos personales por parte de los sujetos obligados, que permitan prevenir la vulneración del derecho.

"El rol debería ser orientador y formulador de iniciativas que alimenten el proceso de política pública sobre el tema".

"Debería haber una suerte de PMG de Transparencia y Anticorrupción a cumplir por los organismos públicos".

"El Consejo debiera tener líneas de asesoría a organismos públicos en el cumplimiento de la ley de protección de datos, para lo cual debiera potenciar su estructura interna con capacidades en esta materia".

En este rol propositivo y orientador al establecer parámetros, se inscribe la idea que se recibió en este proceso consultivo, que plantea la necesidad de desarrollar un esquema socio jurídico que permita ponderar ambos derechos con la finalidad de disminuir la desconfianza en las instituciones públicas.

"Articular un esquema dogmático socio-jurídico interpretativo del derecho a la protección de los datos personales concordado con la obligación de transparencia activa y la política de datos abiertos gubernamentales con enfoque en los derechos fundamentales, a la luz de la legislación, el derecho comparado y, la jurisprudencia, a los fines de armonizar los presupuestos jurídicos relativos al tratamiento de la información pública que permita superar las limitaciones de la desconfianza ciudadana en las instituciones políticas en un contexto de nuevas demandas ciudadanas".

Garante del derecho PDP (1 comentarios)

Se aborda el rol del Consejo planteando que debiera garantizar el derecho de protección de datos personales.

"Es prioritario que se valide como órgano especializado y su rol como garante debiera fortalecerse con el tiempo".

Fiscalizador y sancionador (3 comentarios)

Se considera relevante el rol fiscalizador, sobre todo en la puesta en marcha de la normativa cuando a los sujetos obligados, especialmente del sector privado, les pueda costar más cumplir con la norma, o presenten resistencias a ella, y ante esto debiera sancionar los incumplimientos.

"Respecto a las empresas privadas, un desafío prioritario será la fiscalización. El CPLT tiene experiencia fiscalizando a organismos públicos, que tienen a su vez un deber general de cooperación. Sin embargo, es muy probable que fiscalizar a la industria resulte mucho más complicado. Es posible que se pretenda eludir la fiscalización, y que exista una mayor propensión a litigar demorando la efectividad de las sanciones. Es también probable que exista una inclinación menor a transparentar su funcionamiento interno frente al órgano fiscalizador, en particular respecto de prácticas que se han mantenido en la opacidad por largo tiempo (…) y finalmente en el ejercicio de sus facultades de sanción y la eventual litigación en sede judicial sobre esas sanciones".

"Yo esperaría un órgano que no le tiemble la mano para fiscalizar (focalizadamente), dictaminar y sancionar".

"El principal rol de CPLT, de transformarse en autoridad pública de control de datos personales, será dotar a la legislación de protección de datos personales de efectividad para resguardar el derecho a la autodeterminación informativa (…) en particular a través de actividades de fiscalización, investigación y dictación de sanciones que resulten disuasivas".

IV. Anexos

Anexo 1: Idea propuesta

Idea	Contenido principal de la idea
Antología de Derechos: Derecho de Acceso y Protección de datos personales	Articular un esquema dogmático socio-jurídico interpretativo del derecho a la protección de los datos personales concordado con la obligación de transparencia activa y la política de datos abiertos gubernamentales con enfoque en los derechos fundamentales, a la luz de la legislación, el derecho comparado y, la jurisprudencia, a los fines de armonizar los presupuestos jurídicos relativos al tratamiento de la información pública que permita superar las limitaciones de la desconfianza ciudadana en las instituciones políticas en un contexto de nuevas demandas ciudadanas.

Anexo 2: Respuestas al Formulario

Respuesta	1.Debilidades del Estado en tratamiento de Datos Personales: ¿Qué brechas identifican en los Organismos del Estado para abordar un tratamiento adecuado de los Datos Personales?
1	Educación y capacitación respecto de que se debe entender por Datos personales, marco de responsabilidades que esto implica.
2	No existe en el Estado una libre circulación de datos en las condiciones debidas. Los organismos públicos con competencias para hacer tratamiento de datos son incapaces de generar beneficios públicos porque no lograr crear "las condiciones debidas" para sus circulación lícita. El tratamiento nace y muere en ellos de manera aislada.
3	Fallas de seguridad Ausencia de obligación de políticas de privacidad en los tratamientos de datos personales No hay delegados de protección de datos personales en los órganos del Estado
4	Hay trámites que no indican confidencialidad de los datos, o bien que existen rumores sobre la no confidencialidad. Por ejemplo, denuncias ante la Dirección del Trabajo, es conocido que mucha gente no hace porque se dice que el empleador accede a esos datos. Por otro lado, ciertos trámites no son bidireccionales, es decir el organismo ante el que uno acude muchas veces cierra casos sin satisfacción del usuario (son trámites personales en los que hay tratamiento de datos)
5	Existe muy poco conocimiento de la importancia que tiene el tratamiento de los datos personales . Eso favorece a los organismos del Estado.
6	Falta de capacitación, no hay conocimiento de la normativa, de como aplicarla y como llevarla a la practica más allá de generar documentos. Falta construir puentes entre las areas de negocio, tics y juridicas. Falta de compromiso con la protección de datos desde la más alta dirección, incluso en organismos donde es crítico.
7	La ley actual es bastante letra muerta dado el desconocimiento de sus derechos por parte de la ciudadanía, así como por que no existe una entidad que vele por su cumplimiento, fiscalizando e impartiendo estándares, por lo que varía entre distintos organismos. Hay mucho desconocimiento de la ley por parte de funcionarios también.
8	No existe institucionalidad o esta es difusa y desconocida por la comunidad.
9	Una de las principales brechas emana del error de base de la comprensión de la protección de datos como una excepción a la transparencia en vez de entender que se trata de un derecho autónomo.

	Este error lleva a que se ponga en balance estos dos derechos haciendo primar uno respecto del otro (normalmente la transparencia) con una escasa comprensión de los derechos que se ven vulnerados o se ponen en riesgo por la divulgación de la información. De esta manera, los organismos públicos se encuentran en un debate abierto y permanente derivado de que ellos comprenden "el negocio" y conocen los riesgos de entregar ciertos datos personales, pero no tienen las competencias específicas para exponer sus argumentos frente al Consejo para la transparencia. A vía ejemplar, el caso Nic Chile. La información que consta en el Registro de Nic Chile se transparentó por resolución del Consejo. Esa información permite atacar sitios web (contiene la información de la máquina en que están alojados) extorsionar a sus dueños (secuestrando sus sitios), estafar a terceros (suplantar sitios web), entre otros delitos informáticos. Sin embargo la Universidad de Chile no logró explicar esta situación ante el Consejo ni este comprender las magnitudes del problema. Otro caso ejemplar en su momento fue la entrega de la base de datos de SERVEL, en que constan datos sensibles de las personas.
10	Una primera brecha importante está constituida por la carencia de medidas sistemáticas de seguridad para resguardar la integridad, disponibilidad y confidencialidad de la información personal en poder del Estado, y la necesidad de implementarlas. Estas medidas de seguridad pueden corresponder a mejoras en el diseño de las plataformas digitales y su administración (permisos, privilegios de usuarios), como también de medidas técnicas cuyo objetivo es impedir la filtración, robo, destrucción o mala utilización de la información. En este sentido, los organismos públicos deberán invertir recursos técnicos y humanos para implementar las obligaciones de privacidad por diseño y de seguridad, como las contenidas en el proyecto de ley de datos personales hoy en el Congreso. Estas reglas de seguridad deben también ser aplicadas respecto de las bases de datos hoy existentes, auditando sus contenidos y sus condiciones actuales de seguridad. A ello se suma la necesidad de iniciar evaluaciones de impacto en protección de datos respecto de cualquier iniciativa futura en entidades estatales. En segundo lugar, otra brecha importante tiene que ver con la causal de habilitación para el tratamiento de datos personales por el Estado. Por regla general, el tratamiento de datos personales por parte de organismos públicos tiene como fundamento el artículo 20 de la Ley Nº 19.628, y no el consentimiento del titular. Sin embargo, la utilización en la ley de la expresión “respecto de las materias de su competencia” resulta ambigua, y no entrega parámetros para evaluar de forma más precisa si un organismo público puede o no puede ampararse en esta causal de habilitación. El mismo artículo también establece que este tratamiento debe realizarse cumpliendo con las “reglas precedentes”, lo que significa que aun estando habilitados por el artículo 20, debe cumplirse con los principios de finalidad, proporcionalidad y otros requisitos establecidos por la ley. El proyecto de ley hoy en el Congreso habla de “funciones legales” y no solo competencias da a entender que el estándar para determinar cuando un organismo público estará habilitado para tratar datos personales sin el consentimiento del titular será más estricto. Asimismo, existe un importante vacío normativo en torno a los requisitos, finalidades y condiciones bajo las cuales una entidad pública puede comunicar datos personales con otros órganos del Estado. Esto conlleva un intercambio no regulado adecuadamente, aumentando el riesgo para los titulares de los datos. En general, se ha utilizado la figura de los convenios de colaboración para realizar estos intercambios, lo que no suelen cumplir con establecer una finalidad clara para el tratamiento de los datos, verificar que el organismo receptor esté habilitado expresamente por ley para procesarlos, y establecer medidas de seguridad y eliminación segura de estos datos, además del cumplimiento continuo de las obligaciones de seguridad. Como consecuencia, y sumado a los puntos anteriores, existe un riesgo alto de tratamiento de datos personales por órganos públicos, no autorizado por ley ni por los titulares, con comunicación entre distintos órganos bajo condiciones de dudosa legalidad, sin fiscalización ni garantías de protección, y sin garantías de calidad ni de

	eliminación oportuna.
Respuesta	**¿Qué riesgos en materia de discriminación hacia las personas y/o grupos sociales conlleva un tratamiento deficiente de Datos Personales? ¿Cómo debieran ser abordados estos riesgos?**
1	capacitación en lenguaje claro del derecho constitucional,
2	El riesgo más evidente es el de tratamiento de datos caducos o desactualizados. Otro riesgo importante es el acceso indebido y la falta de sanciones asociadas al acceso ilegal. Si esta circunstancia no se sanciona queda en la atmósfera la sensación que no existe igualdad ante la ley y se incrementa la percepción de corrupción.
3	El Estado recoge datos especialmente de personas pertenecientes a grupos vulnerables o grupos desaventajados y los somete a tratamientos altamente intrusivos. Ejemplo: reconocimiento biométrico en raciones de comida JUNAEB.
4	Estigmatización a grupos vulnerables, violencia en redes sociales, publicación masiva, etc. Estos actos pueden ser realizados por personas, como por instituciones (conocidos casos de amenazas en redes por parte de fuerzas de seguridad).
5	Riesgos de discriminación en cuanto al acceso al empleo, a la educación y a la salud, fundamentalmente. Pero también en cuanto al ejercicio de los derechos civiles y políticos. El primer paso es una campaña de educación para que la ciudadanía comprenda que el tratamiento de los datos personales tiene implicancias sociales, políticas y de derechos humanos.
6	Creo que estos riesgos se abordan más allá de la normativa misma. Siempre es útil un análisis de impacto previo para determinar por ejemplo, aspectos relacionados con la calidad de dato o la seguridad que pudieran generar discriminaciones u otras consecuencias indeseables en las personas. Los riesgos deben evaluarse antes del tratamiento y no solo considerar la normativa de privacidad sino aspectos éticos que hoy también son relevantes.
7	Sin comentario
8	Los mayores riesgos que se aprecian son las denominadas funas que quedan en la impunidad al relativisarse lo privado y personal en beneficio de la publificacion de todo y asignarle a la publicidad un valor moral y mayor protección jurídica que a la vida privada. Hay un desbalance entre lo público y lo privado.
9	Es una visión sesgada pensar que el tratamiento de datos personales abusivo se reduce a la discriminación de las personas. El riesgo alcanza a todos y cada uno de los derechos de las personas. Baste el ejemplo a que se aludió antes, en que el derecho de propiedad, la seguridad personal, la seguridad nacional, etc., se puede ver afectada por la entrega indiscriminada de la base de datos de Nic Chile. Por tanto los riesgos en relación a los derechos de las personas por el tratamiento abusivo de los datos personales se morigerarían si existiera una autoridad independiente, técnica y con atribuciones suficientes como para comprender las lógicas del tratamiento de datos personales, con una integración multidisciplinaria que pudiera ponderar cada caso, asesorar a quienes hacen tratamiento de datos en la correcta aplicación de la ley en sus operaciones de tratamiento, educar a la población en la persecución de sus derechos, entre otras garantías institucionales.
10	En primer lugar, constituye una forma de “tratamiento deficiente” la que implica una recolección desproporcionada de información personal, incluida la no relacionada con el giro de quien la solicita ni con la necesidad de identificar a las personas (como en la exclusión por nacionalidad o lugar de residencia). Esto ocurre en un primer nivel con la solicitud de información vinculada a la identificación frente al Estado, y luego con la recolección de información biométrica. Sumados a

	otras prácticas de recolección extensiva y de perfilamiento, bajo dudosas condiciones de consentimiento informado, convierten al tratamiento de datos personales en un mecanismo cada vez más avanzado para la exclusión social. En segundo lugar, la convivencia social ya se ha visto afectada históricamente mediante las prácticas de perfilamiento a partir de puntajes de sistema de riesgo crediticio en mercados o para operaciones no directamente relacionadas. El ejemplo histórico de la exclusión por "estar en DICOM" se mantiene en la medida en que no se ilegaliza la exigencia a las personas de exhibir ese puntaje (cuando no puede ser obtenido por la posible contraparte en el otorgamiento de un servicio). El intercambio de bases de datos personales sin base legal ni consentimiento informado que conlleva este riesgo, es también una práctica de tratamiento deficiente. Otro riesgo está vinculado a la recolección de datos conductuales, historial de compras u otros datos relativos a los hábitos de las personas, junto con la creación de datos inferidos, con la finalidad de perfilar a los usuarios. A medida que el comercio detallista, el sector financiero y otros sectores económicos echan mano a estos mecanismos para realizar publicidad dirigida o determinar el precio de primas de seguros, aumenta el riesgo que este perfilamiento o encasillamiento sea utilizado de forma arbitraria o discriminatoria. Este resultado puede producirse por distintas razones: puede existir un perfilamiento errado, o recolección de información desactualizada, o de información reservada o no atingente (por ejemplo, realizar un análisis de las redes sociales del cliente para efectos de cálculo de riesgo crediticio), con el resultado buscado o no de discriminar a individuos de ciertos grupos. Por otro lado, el uso de técnicas más avanzadas de análisis algorítmico acarrea el riesgo de resultar en resultados sesgados, arbitrarios o discriminatorios. Estos mecanismos pueden reproducir o incluso profundizar los sesgos implícitos de quienes los diseñan, programan o utilizan, ya sea en la selección de los datos, la ponderación que se le entrega a cada variante, o la calidad de los datos mismos. Estos sesgos pueden ser extremadamente difíciles de detectar, porque el análisis de datos goza de un aura de aparente neutralidad, y porque los algoritmos pueden estar exentos de auditoría y protegidos por distintas figuras de propiedad intelectual. Es necesario que una futura autoridad pública de control cuente con suficientes atribuciones jurídicas, capacidad técnica y recursos humanos para llevar a cabo una fiscalización efectiva de estos mecanismos de recolección y análisis de datos. Una alternativa es que los responsables de bases de datos tengan la obligación de reportar a la autoridad de control cuáles fueron las medidas que tomaron para evitar que sus algoritmos vulneren bienes jurídicos que como sociedad consideramos relevantes, como la igualdad en dignidad y derechos. Las evaluaciones de impacto de protección de datos en los términos del RGPD europeo es un mecanismo que sirve a parte de estos fines.
Respuesta	**¿Cuál debiera ser el Rol del CPLT como garante de la PDP? ¿Cuáles debieran ser sus líneas de acción prioritarias y públicos objetivos?**
1	El CPLT podría dirigir sus programas de capacitación al público o usuario. Desarrollo de programas de difusión por etapas (planificación estratégica con indicadores y verificadores claros) socialización de resultados. Identificar las deficiencias materiales para su aplicación
2	No estoy de acuerdo con que desarrolle esta función. En el evento que asuma esas atribuciones y suponiendo que habrá una vacancia entre la entrada en vigencia de estas normas, pienso que el CplT debería trabajar fuertemente en prevención, en alentar a los sujetos obligados a reducir al máximo el almacenamiento de datos de manera que los responsables del tratamiento entiendan que mientras menos datos traten o administren, menor será su responsabilidad. En el caso del sector público, creo es importante trabajar en protocolos internos y de intercambio de información que es

	donde existe el mayor desafío entrefinos de transferencia segura de información personal.
3	Rol: Promotor del derecho, auditoría y fiscalización, regulador. Líneas prioritarias: Salud, educación y beneficios sociales.
4	Creo que un buen benchmarking con políticas asociadas en países avanzados en esta materia sería positivo. Que se apliquen en Chile las buenas prácticas levantadas a nivel global. Aplicar con énfasis en el caso chileno: alta desconfianza en instituciones públicas y privadas.
5	Para que el CPLT se requiere un estrecho vínculo con la sociedad civil y el resguardo riguroso de su autonomía. Debería haber una suerte de PMG de Transparencia y Anticorrupción a cumplir por los organismos públicos y una campaña nacional respecto del tema. Aún hay muy poca cultura respecto de que la PDP es un asunto de derechos humanos.
6	Hoy en mi opinión el rol de Consejo ha sido relevante pero a la vez timido. Se ve comunicacionalmente mucho, pero en la practica podría hacer mucho más con el "velar por" del 33m). Como desafíos de gestión al futuro es prioritario instalar culturalmente la protección de datos en la organización. El Consejo es un órgano de transparencia y ya sabemos que la PDP no es la otra cara. Es mucho más amplia y desafiante pues involucra al sector privado. Es prioritario que se valide como organo especializado y su rol como garante debiera fortalecerse con el tiempo. Yo esperaría un órgano que no le tiemble la mano para fiscalizar (focalizadamente), dictaminar y sancionar. Sus lineas de acción al comienzo debieran ser difusión y su publico objetivo debiera ser el ciudadano, sin perjuicio de las guías y todo el material de apoyo que debería ser capaz de generar, ojalá actuando de manera proactiva y no reactiva. Hoy el Consejo reacciona en los medios cuando ve injusticias, pero no se ve una política de acción y propositiva que podría explotar aún más.
7	Hoy el Consejo tiene una mínima potestad al respecto, pero circunscrita al sector público, sin embargo sin facultades ni muchas capacidades para realmente ejercer dicho rol. Por esto, es necesario que se avance en esta materia, ya sea dándole la competencia al Consejo (mi primera opción) u a otra entidad autónoma. Si es el Consejo, es necesario avanzar en ciertas materias en su gobierno corporativo así como tambien en ciertos equilibrios y rendición de cuentas
8	El rol debería ser orientador y formulador de iniciativas que alimenten el proceso de política pública sobre el tema
9	En primer lugar, aun sin ley adecuatoria, el Consejo debiera dar una aplicación correcta a la atribución de "velar" por la correcta aplicación de la ley 19.628. Si bien a la fecha han realizado algunos esfuerzos, en sus resoluciones no se aprecia que se haya comprendido el alcance de este derecho ni los riesgos que entraña para la persona la circulación indiscriminada de datos a partir de la entrega incausada de datos que constan en poder de la administración. Esto podría lograrse haciendo educación al interior del consejo (a los consejeros) y a los organismos públicos en la comprensión que deben traspasar al Consejo para que éste pueda resolver correctamente los asuntos en que hay datos personales comprometidos. Generar espacios de reflexión al interior del consejo. En su composición, debiera haber consejeros que adhieran a los principios y normas de protección de datos, que sean capaces de entender los aspectos técnicos del tratamiento de datos. El Consejo debiera tener líneas de asesoría a organismos públicos en el cumplimiento de la ley de protección de datos, para lo cual debiera potenciar su estructura interna con capacidades en esta materia.
10	El principal rol de CPLT, de transformarse en autoridad pública de control de datos personales, será dotar a la legislación de protección de datos personales de efectividad para resguardar el derecho a la autodeterminación informativa. Para ello deberá contar con las atribuciones legales y las facultades sancionatorias que le permitan hacer efectiva la normativa, en particular a través de

	actividades de fiscalización, investigación y dictación de sanciones que resulten disuasivas. Además deberá contar con los recursos económicos, técnicos y humanos para estos propósitos. Respeto a las acciones prioritarias del CPLT cuando se transforme en el órgano encargado de velar por el cumplimiento de la normativa de PDP, es necesario distinguir entre los órganos sujetos a su control. Respecto de su labor de fiscalización de otros organismos públicos, deberá ser una prioridad la fiscalización de las medidas de seguridad, así como el control en la cesión de datos a otros organismos públicos y privados. Deberá crear lineamientos y protocolos para la gestión de información personal, incluida la comunicación de datos entre distintas entidades. Respecto de los organismos privados, la autoridad de control deberá establecer pautas claras que impidan a distintas industrias realizar recolección y tratamiento masivos e indiscriminados de datos personales. Para ello, el control y establecimiento de parámetros para que los titulares entreguen su consentimiento de forma expresa, previa e informada será central, así como también la formulación de estándares que sirvan a las propias empresas para adecuar su acción a las obligaciones legales y las expectativas de la autoridad. También con respecto a las empresas privadas, un desafío prioritario será la fiscalización. El CPLT tiene experiencia fiscalizando a organismos públicos, que tienen a su vez un deber general de cooperación. Sin embargo, es muy probable que fiscalizar a la industria resulte mucho más complicado. Es posible que se pretenda eludir la fiscalización, y que exista una mayor propensión a litigar demorando la efectividad de las sanciones. Es también probable que exista una inclinación menor a transparentar su funcionamiento interno frente al órgano fiscalizador, en particular respecto de prácticas que se han mantenido en la opacidad por largo tiempo. Existe un desafío significativo y prioritario en el desarrollo de capacidades para el ejercicio de las labores propias de una autoridad de control. Se requiere énfasis en las funciones educativa, interpretativa y de fijación de estándares por parte de la autoridad de control, como también en la capacidad negociadora para llegar a acuerdos que permitan protección y reparación oportunas en casos de infracción, y finalmente en el ejercicio de sus facultades de sanción y la eventual litigación en sede judicial sobre esas sanciones. Se requerirá priorizar la comunicación al público general, como también producir material adecuado a operadores clave del sistema, tanto del ámbito privado como público, expandiendo esfuerzos realizados hasta ahora. Se requerirá un involucramiento significativo con entidades estatales en el ámbito de la ciberseguridad a fines de alinear prioridades y objetivos. Finalmente, se deberá expandir el trabajo de involucramiento regular de las múltiples partes interesadas en la protección de datos personales, para la formación de políticas de la autoridad hacia el futuro y su evaluación.