HIPER DERECHO

Tecnología como libertad

Lima, 10 de septiembre de 2019

Señor
Martín Vizcarra Cornejo
Presidente de la República
Presente. —

Asunto: Comentarios a la Autógrafa de Ley de Ciberseguridad aprobada por el Congreso de la República

Hiperderecho es una asociación civil peruana sin fines de lucro dedicada a investigar y promover el respeto de los derechos humanos en entornos digitales, conformada por abogados y especialistas en tecnología. Como parte de nuestro trabajo, estudiamos todas las iniciativas de política pública que puedan impactar el ejercicio de derechos y libertades en estos ámbitos.

En esta ocasión nos gustaría ofrecer comentarios relacionados a la Autógrafa de la Ley de Ciberseguridad que la Comisión Permanente ha presentado a su despacho el 20 de agosto de 2019 (en adelante, la "Autógrafa"). Nuestra finalidad es que estos comentarios se sumen a los aportados por otras entidades públicas y privadas y le sirvan como apoyo para calificar si esta norma merece su aprobación y promulgación o la observación y vuelta al Congreso.

1. Es necesario observar la Autógrafa de la Ley de Ciberseguridad

Consideramos que es necesario que su despacho observe la Autógrafa de la Ley de Ciberseguridad por múltiples razones de forma y fondo, siendo las más importantes:

(i) La Cuarta Disposición Complementaria Final de la Autógrafa señala (de forma errada) que el Ministerio del Interior es el ente rector de la seguridad digital en el país, pese a que hasta en dos leyes anteriores esta rectoría se ha asignado a la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros;

(ii) Existen varios artículos en la Autógrafa que establecen obligaciones en materia de seguridad digital para actores públicos y privados cuya redacción es vaga y admite múltiples interpretaciones, algunas de ellas contradictorias, lo que puede generar inseguridad jurídica;,

(iii) En su artículo 5, la Ley crea una "Comité de Ciberseguridad del Estado Peruano" que estaría conformado por entidades públicas y privadas, pero al cual se le han asignado facultades y competencias que van más allá de lo que el Congreso está facultado a otorgar a través de una Ley, lo que lo hacen inviable y afecta la eficacia de toda la norma.

Los problemas identificados son insubsanables en la instancia procesal en la que se encuentran actualmente. Por lo tanto, la única vía por la cual pueden ser revisados y corregidos por sus proponentes es que el Presidente de la República observe la norma y esta sea devuelta al Congreso.

Como una organización comprometida con la defensa de los derechos humanos en entornos digitales, creemos que contar con una Ley de Ciberseguridad es necesario para la madurez de nuestro ecosistema digital. Precisamente por eso nos preocupa que se apruebe un texto con errores de forma y fondo que pueden terminar entrampando el desarrollo de nuestro país en este espacio.

2. Sobre la rectoría de la seguridad digital en el país

La Cuarta Disposición Complementaria Final de la Autógrafa de Ley señala explícitamente que:

> CUARTA: Desarrollo del currículo de educación superior en materia de ciberseguridad: El Ministerio del Interior, en su calidad de ente rector en materia de seguridad digital coordina con el Ministerio de Educación, la pertinencia del desarrollo de contenidos especializados en materia de seguridad digital, que incluye la ciberseguridad en las instituciones de educación superior universitaria y tecnológica, a nivel de pre y postgrado. Para ello, establece instrumentos de cooperación interinstitucional con entidades del sector privado, la academia, la sociedad civil y la comunidad técnica. *(El subrayado es nuestro)*

Señalar que el Ministerio del Interior tiene dicha rectoría es un error. Primero, porque dicha rectoría ya ha sido asignada a la Secretaría de Gobierno Digital hasta en dos leyes actualmente vigentes: La Ley N° 30999 (“Ley de Ciberdefensa”) y el Decreto Legislativo N°1412 (“Ley de Gobierno Digital”). Segundo porque ni en el contenido de la Ley ni en su Exposición de Motivos se hace explícita la intención de realizar un cambio de rectoría. Tercero porque, de aprobarse la Autógrafa con este cambio, se producirá inmediatamente un grave conflicto de competencias en el Estado, que afectarán el desarrollo no solo de la seguridad digital sino también de los planes de gobierno digital actualmente en marcha.

Ya sea que exista un error material o que se haya dispuesto este cambio de forma deliberada, consideramos que aprobar un cambio de rectoría de esta forma es contraproducente para cualquier avance en materia de seguridad digital y va en contra de los intereses del país. Si su despacho atiende este comentario, debería observar la Autógrafa de Ley y solicitar la modificación de este párrafo en específico.

3. Sobre la vaguedad en la creación de obligaciones para actores públicos y privados

A lo largo de toda la Autógrafa, es posible encontrar múltiples ejemplos de redacción informal, intercambio contínuo de términos entre artículos y, en algunos casos, expresiones vagas, genéricas o mal fraseadas al punto en que se pueden extraer varias interpretaciones, incluso contradictorias.

El ejemplo más grave es el artículo 4, inciso 2, que dice así:

Artículo 4.— Principios de la ciberseguridad

4.1. Comunicación de incidentes: Se deberá crear mecanismos de comunicación de incidentes entre la sociedad civil, el sector privado, la academia, la comunidad técnica y el sector gubernamental. Dichos mecanismos de comunicación de incidentes deberán mantener la reserva de los casos indicados, en los casos que pudiera su revelación afectar a las instituciones o a la sociedad, pero también deberá evaluarse los casos para divulgar dicha información a otros actores y a la sociedad. Tanto el compartimentaje como la diseminación de la información a los organismos pertinentes no debe afectar la defensa o la seguridad nacional.
En el caso de que los incidentes impliquen violación a datos personales deberá informarse al funcionario público responsable de transparencia y acceso a la información pública y a la protección de datos personales, de dicha afectación.

De igual manera los incidentes deberán ser reportados ante las autoridades competentes de acuerdo a la naturaleza de la entidad vulnerada y de los individuos y entidades afectadas, para que respondan a dicha afectación en la medida de sus funciones. *(El subrayado es nuestro)*

Como se desprende del texto resaltado, el lenguaje empleado es ambiguo y la longitud de las oraciones, en donde se acumulan múltiples obligaciones y supuestos en abstracto no permite discernir bien la intención del texto. Por ejemplo, respecto de los mecanismos de comunicación de incidentes, no se señala a qué se refieren exactamente con ellos (¿Los CSIRT? ¿Los protocolos para reportar los incidentes? ¿El canal por donde se hacen los reportes?). Tampoco existe claridad respecto de a quiénes alcanzan las obligaciones de reporte y reserva (¿Al CSIRT? ¿A las entidades afectadas? ¿A todo el que conociese del caso?)

También, en el párrafo donde se habla de incidentes que impliquen “violación a datos personales,” se hace referencia al deber de comunicar estos al funcionario encargado de transparencia, acceso a la información pública y protección de datos personales. Existen dos problemas con esta redacción. En primer lugar, no existe un funcionario con ese título. Lo que existe actualmente es un funcionario de transparencia en cada institución del Estado, cuya función es asegurarse de que se contesten las solicitudes de acceso a la información y se publique información pública en los portales del Estado. En segundo, asumiendo que la norma se refiere a dicho funcionario ¿cuál es el propósito de notificarle los incidentes? Por simple lógica, consideramos que lo que se ha querido hacer es invocar a la Dirección Nacional de Protección de Datos Personales, que tiene todas las competencias necesarias para ocuparse de las consecuencias de estos incidentes cuando afecten datos personales. No obstante, la redacción está tan alejada de esta idea que aun si el Reglamento quisiera corregirla, esto iría más allá de lo que dice la ley, lo que supone una causal de inconstitucionalidad directa.

Si su despacho atiende a este comentario, debería observar la Autógrafa de Ley y solicitar la modificación de este inciso con el fin de que se ejecute una redacción más clara y concisa en donde las obligaciones y los obligados se encuentren bien delimitados, así como las atribuciones de entidades públicas tales como la Autoridad de Protección de Datos

Personales. De no hacerlo, se atenta contra la seguridad jurídica, especialmente de las entidades del sector privado, lo que redundará en la inefectividad de esta norma.

4. Sobre el Comité de Ciberseguridad y su inviabilidad

En su artículo 5, la Autógrafa de Ley propone la creación del Comité de Ciberseguridad del Estado Peruano en los siguientes términos:

> Artículo 5.— Comité de Ciberseguridad del Estado Peruano
>
> Dispóngase la creación del Comité de Ciberseguridad del Estado Peruano, el mismo que deberá contar en su conformación con participación del sector privado, sociedad civil, academia, comunidad técnica de Internet y sector gubernamental. Este comité estará adscrito a la Presidencia del Consejo de Ministros y la Secretaría de Gobierno Digital será la secretaría técnica, quien coordinará con el secretario técnico del Consejo de Seguridad y Defensa Nacional (COSEDENA).
>
> El Comité Tendrá como función formular la Política de Ciberseguridad del Estado Peruano, generar lineamientos en materia de CSIRT en el sector privado, gestionar el Fondo de Seguridad Digital, fomentar la cultura de ciberseguridad, coadyuvar al fomento de currículos de educación superior en materia de ciberseguridad y otras que les pudiera establecer la COSEDENA.
>
> La conformación del Comité de Ciberseguridad del Estado Peruano será establecida en el reglamento de la presente ley.

Es muy positivo que se incluyan a los actores del sector privado como parte de un organismo de ciberseguridad nacional, siguiendo un modelo recomendado por múltiples instancias internacionales y en reconocimiento del carácter multi estamentario del entorno digital.

No obstante, notamos que existen varios elementos que hacen del Comité una propuesta inviable y contraria al ordenamiento legal vigente. Por ejemplo, se menciona que una de las funciones de este órgano es la de gestionar el Fondo de Seguridad Digital. No obstante, el artículo 79 de la Constitución Política ordena que el Congreso no tienen iniciativa para crear ni aumentar gastos públicos. Esto significa que no es posible crear dicho fondo por ley, una facultad exclusiva del Ejecutivo. Además, un organismo conformado por públicos y privados de esta naturaleza tampoco tendría capacidad para ejecutar presupuesto alguno, asumiendo que se le asigne, ni un personal propio para administrarlo.

La experiencia internacional permite ver que, cuando un país desarrolla una estrategia, plan o ley nacional de ciberseguridad, una buena práctica es asegurar la participación del sector privado (sociedad civil, empresas, etc.), pero esto suele ser a través de la creación de órganos de seguimiento, observatorios, mesas de trabajo u otros espacios análogos. No obstante, las decisiones ejecutivas y presupuestales permanecen en el Estado y no existe actualmente un modelo dentro del marco legal peruano que permita la creación de un órgano como el Comité de Ciberseguridad propuesto.

Conscientes de la necesidad de institucionalizar la participación del sector privado, especialmente de la sociedad civil, en la creación e implementación de las políticas nacionales de seguridad digital, no podemos dejar de decir que proponer una solución de participación inviable es tanto igual o peor que no proponer ninguna. En ese sentido, si su despacho atiende a este comentario, debería observar la Autógrafa de Ley y solicitar la modificación total de este artículo, debiendo cambiar la estructura del Comité o restringir sus facultades con el fin de que se adecue a la Constitución y sus normas de desarrollo.

5. Otros errores de redacción

Además de los ya mencionados, existen otros cambios accesorios que deberían hacerse a la Autógrafa de Ley con el fin de que mejore su capacidad de producir efectos positivos en materia de seguridad digital. Algunos son de tipo formal. Por ejemplo, en los artículos 4 y 5 se hace mención en dos ocasiones a "la Comunidad Técnica" y luego a la "Comunidad Técnica de Internet". Esto debe ser modificado con el fin de uniformizar el lenguaje de la norma pues es evidente que se ha intentado mencionar al mismo grupo de interés pero se han utilizado diferentes nombres, lo que podría generar confusión.

Otro caso es el de la definición de los CSIRT. La definición ofrecida en el artículo siete hace referencia al PeCSIRT, que describe como el centro de atención de emergencias nacional en materia de seguridad digital. Este artículo es problemático en tanto ya existe una entidad nacional que coordina los esfuerzos sobre atención de emergencias en las redes informáticas del Estado: El PeCERT. Si bien ambos nombres son intercambiables porque básicamente la descripción del PeCSIRT es análoga a la del PeCERT, no queda claro si este artículo significa la disolución del PeCERT o simplemente su cambio de nombre.

Estos problemas no resultan críticos y podrían superarse en la fase de reglamentación de la ley o mediante una Fe de Erratas. Sin embargo, sumados a los problemas graves ya identificados en secciones anterior, nos hacen solicitar a su despacho que considere la observación de esta ley y su devolución al Congreso para que se realicen las modificaciones necesarias.

Por todo lo expresado, solicitamos a su despacho que observe la presente Autógrafa de Ley de Ciberseguridad para que sea devuelta al Congreso y puedan ser subsanados los problemas identificados.

Atentamente,

Miguel Morachimo Rodríguez
Director Ejecutivo

Carlos Guerrero Argote
Director de Políticas Públicas