Fundación Datos Protegidos

Propuesta de SUBTEL	Comentarios FDP
Artículo 1	Limitar norma a "envío de información sobre ciberincidencias" deja fuera el actuar habitual o prácticas de los operadores, y en particular un tema clave de 5G y de creciente importancia en general: datos que se generan a partir del comportamiento de usuarios. Esta limitación incluso contradice mención del artículo 2 párrafo "a" que refiere a "interacciones sociales" y párrafo "b" sobre "confidencialidad de los datos almacenados"; se trata de datos necesarios de proteger, tanto en sí mismos como en cuanto a datos de segundo orden derivados a partir de ellos, o de cruces de ellos con otros. La norma debe establecer de manera más explícita la obligación de proteger todos los datos generados por usuarios, incluyendo metadatos y contenidos, los que deberían ser eliminados de los sistemas de los operadores a penas su uso no sea necesario, y solamente almacenarse y entregarse por orden judicial y bajo supervisión de un juez de garantía, esto puesto que los metadatos y datos de tráfico de usuarios pueden revelar ubicación, comportamiento, comunicaciones y categorías definidas como datos sensibles en la actual ley 19628. También, es necesario que ciberincidencias se puedan reportar por terceros, no solamente "concesionarios y permisionarios", esto no solamente porque dichas empresas puedan tener conflictos de interés, también porque los usuarios son quienes tienen el mayor interés y son una efectiva superficie de contacto para la detección de problemas que les afectan, por ejemplo incidencias de fallas en la disponibilidad del servicio contratado. También, estamentos del Estado deberían poder supervisar y reportar ciberincidencias, siendo un contrasentido que la misma Subsecretaría de Telecomunicaciones y futuros estamentos relacionados con ciberseguridad no pudieran hacerlo.

Artículo 2	La definición de "riesgo" (letra i) es limitante a "seguridad". Esta definición debería incluir también privacidad explícitamente, pues a través de estas redes circulan datos personales y sensibles, sería un contrasentido que su protección quede fuera de una norma de ciberseguridad. Si bien se puede entender en algunos contextos que la privacidad está contenida en la “seguridad”, esto no es consensual, ni siquiera a nivel regulatorio, por lo cual cabe la precisión.
Artículo 3	Puede que limitar a "servicios de telecomunicaciones" sea un error, toda vez que ciberseguridad también abarca la prestación de servicios no relacionados con conectividad per se.
Artículo 4	En conexión con el punto anterior, la definición de "operador relevante" podría ampliarse a algunos operadores de misión crítica más allá de las redes mismas. Como ejemplo: se podría argüir que servicios como mensajería, mapas, e-mail, pago de cuentas online y otros trámites pueden resultar tan importantes como las redes mismas, pensando en "Impacto social o económico de eventuales interrupciones". Ello está actualmente relevado por la pandemia.
Artículo 5	El título debería sumar la palabra privacidad, no solamente seguridad, en concordancia con lo que expresamos en relación al art. 2, o al menos explicitar que privacidad está incluído en seguridad. Similarmente, en "k" incluir explícitamente el concepto de privacidad junto al de seguridad. También en "h" podría ser bueno precisarse qué normas y estándares internacionales. Hace falta también en la lista una mención explícita sobre protección de datos, por ejemplo "m) confidencialidad y

	privacidad de datos y metadatos generados por usuarios".
Artículo 7	La norma se centra en obligación de proveedores de automonitorearse, excluyendo la posibilidad de monitoreo de parte de la autoridad, siendo que es bastante sencillo y de bajo costo monitorear al menos continuidad operativa / disponibilidad. No hay razones técnicas por las cuales las incidencias, en especial de interrupción de servicios, no puedan ser informadas casi en tiempo real y de manera automática. El monitoreo de este tipo es muy barato y altamente automatizable. Los reportes de brechas de datos personales se ha establecido en un plazo máximo de 72 horas en el Reglamento Europeo de Protección de Datos y es el mismo plazo previsto en el proyecto de ley de datos personales chileno, y también es el mismo plazo de horas contemplado en la modificación de la ley del consumidor y que fue aprobado con fecha 16 de junio de 2020 (segundo trámite constitucional).
Artículo 13	Parece existir una confusión entre datos personales y datos sensibles en este punto. Los datos personales pueden ser pertinentes de compartirse, los datos sensibles, definidos en la ley 19628 art 2 letra "g" como "aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual" no deberían estar presentes en reportes de este tipo, no se entiende la necesidad ni se justifica la posibilidad de incluirlos, toda vez que incluirlos podría generar riesgo asociados a la discriminación.

Artículo 16.	Nuevamente en este punto, podría ser pertinente precisar qué estándares internacionales. También, llama la atención en este punto que lo precisado en el “a lo menos” parece apuntar solo a la continuidad operativa, en tanto no se ve, por ejemplo, una mención específica sobre pruebas y prevención de spoofing, vale decir que un usuario pueda suplantar a otro, y de ataques tipo “man in the middle”, que también es una forma de suplantación, que hace posible interceptación de tráfico. La suplantación de usuarios o de elementos de la infraestructura son incidencias habituales y claves asociadas a la ciberdelincuencia y por lo tanto debería estar enfatizada la supervisión, detección, pruebas y acciones de protección para minimizar, mitigar o evitar la suplantación a través de las redes de los operadores, y la información a clientes afectados en caso de detección.

Artículo 17.	Se presenta un poco vaga la definición de que la autoridad "podrá fiscalizar". Esta es la oportunidad para definir compromisos de fiscalización más precisos, y que movilicen al organismo a implementar al menos una sencilla estación de monitoreo de disponibilidad, que adicionalmente puede servir para monitorear, por ejemplo, disponibilidad y uso de redes Wi-Fi públicas, enlaces entre proveedores, puntos de intercambio de tráfico y otros servicios críticos conectados. Esto excede el tema específico del reglamento, pero es interesante señalar que existe un sistema ampliamente utilizado por proveedores de conectividad llamado WhatsUp Gold (ninguna relación con WhatsApp), un software además cuya operación es ampliamente conocida por especialistas del ámbito y que por lo tanto no reviste gran dificultad para su puesta en marcha.