La prevención de delitos informáticos en la legislación boliviana, frente a una sociedad generalizada como altamente vulnerable por el retraso digital

Victor Hugo Aranibar
Cochabamba, Junio de 2016

1. Introducción

La tecnología informática evoluciona de forma desproporcionada con relación al aprovechamiento de sus beneficios. La oferta de prestaciones y servicios informáticos sobrepasan considerablemente la satisfacción de las demandas de usuarios. Por su parte, los sistemas de regulación legal no pueden acomodarse al fuerte dinamismo de la evolución computacional, lo que origina una serie de escenarios adecuados y propicios para los ciber delincuentes.

La seguridad informática no es lo suficientemente sólida como para prevenir de las amenazas y delitos informáticos que afectan a usuarios y sociedades enteras. La realidad ciudadana y normativa de Bolivia corresponde a uno de estos escenarios; en la que no existe el suficiente respaldo jurídico normativo como para sobrellevar todas las vulnerabilidades a las que los usuarios computacionales se exponen.

Lo que se hace en esta oportunidad, es contraponer un análisis del marco normativo referido a los delitos informáticos en el país, frente al grado de vulnerabilidad que refleja la realidad boliviana.

2. Avance en la construcción de un marco legislativo para la seguridad informática en Bolivia

Si bien todo sistema legislativo y normativo referido a un determinado campo, atraviesa por un proceso de construcción que acompaña su evolución; para el caso de la informática en Bolivia aún se tiene un acompañamiento jurídico poco nutrido.

En esta oportunidad se han identificado y trabajado once disposiciones legales que tienen implicancia directa o indirecta con la delincuencia informática: Decreto Supremo Nº 27329 “Transparencia y Acceso a la Información”, Ley Nº 164 “Ley General de Telecomunicaciones y Tecnologías de Información y Comunicación”, Ley Nº 341 “Ley de Participación y Control Social”, Decreto Supremo Nº 1391 “Reglamento a la Ley Nº 164”, Decreto Supremo Nº 1793 “Reglamento para el Acceso, uso y Desarrollo de las Tecnológicas de Información y Comunicación”, Ley Nº 650 “Agenda Patriótica 2025”, Decreto Supremo Nº 2514 “Creación de la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación”, Ley Nº 777 “Ley del Sistema de Planificación Integral del Estado SPIE”, Ley Nº 779 “Desburocratización para la creación y Funcionamiento de Unidades Económicas” y el Decreto Supremo Nº 0667 “Código de Procedimiento Penal”.

2.1. Decreto Supremo N° 27329 "Transparencia y Acceso a la Información"

Aunque con una visión de Estado, con el D.S. Nº 27329 se inician las pautas hacia el camino de constitución de un cuerpo normativo especifico a las Tecnologías de Información y Comunicación (TIC) en Bolivia. En esta disposición se resalta la necesidad de disponer de una Ley general de acceso a la información; así también, de procurar una normativa que permita la transparencia y acceso a la información gubernamental por parte de la ciudadanía.

Así como en el D.S. Nº 27329 se involucra al acceso a la información por las personas, también se trata sobre la necesidad de considerar algún tipo de información como clasificada; entre varias como la financiera, y la correspondiente a la delincuencia, lo ilícito y criminal, como para hacer seguimientos y dar con delincuentes –los que en este caso pueden ser informáticos–.

2.2. Ley N° 164 "Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación"

Constituye una Ley General, y dirigida específicamente a la informática –pero no aborda los delitos informáticos–, en la que se analizan ampliamente los procesos de uso de la tecnología y se regula su aprovechamiento lícito y sus implicancias ilícitas, en resguardo de los derechos y obligaciones de las personas en el país.

Son relevantes las muchas definiciones técnicas sobre informática que se hacen en la disposición, aunque no existe ninguna sobre la delincuencia digital o informática; por lo que llama la atención la falta de enunciación de alguna competencia de Estado respecto a la delincuencia o delitos informáticos. Sin embargo, en la Ley Nº 164 se trata de políticas, beneficios y ámbitos de aplicación técnicos de la informática en la vida nacional. Es importante el detalle de aspectos técnicos que se hacen en la disposición –como la regulación de espectros radio magnéticos, sin considerar sus posibles acciones ilícitas–, presentándose muchos aspectos técnicos de manejo, regulación y alcance de los servicios satelitales por ejemplo.

En el Capítulo Quinto –Contratos–, se menciona sobre la protección de los derechos de usuarios y de los datos personales. También se trata acerca la realización de comercio electrónico dentro ambientes técnicamente confiables; evidenciando las posibilidades de pasarse a la justicia ordinaria en caso de controversias.

Por otro lado, se regula sobre los derechos de creación, transmisión, recepción y almacenamiento de correo electrónico; dentro lo que se mencionan sus infracciones y sanciones considerando los criterios de: *naturaleza y gravedad del hecho, extensión y magnitud del peligro o daño causado, dolo o culpa en la comisión de la infracción, existencia de agravantes y atenuantes en la comisión de la infracción*; y entre las infracciones: *apercibimiento, secuestro o embargo de equipos y material; multas e*

inhabilitación temporal para ejercer actividades referidas a telecomunicaciones y TIC, cesación de los actos por el infractor, resarcimiento de daños y perjuicios establecidos judicialmente –igualmente medidas de apercibimiento o llamadas de atención por escrito a los infractores si el hecho es ilícito y se conmina–.

Puntualizando, respecto al secuestro de equipos, componentes, piezas y materiales; dentro la Ley Nº 164 esta acción se considera como una medida precautoria que debe apoyarse en un reglamento, realizarse bajo inventario, y siempre y cuando no se afecten a terceros. Al respecto, la clasificación de las infracciones son: *prestación o ejercicio ilegal de un servicio, accionar contra un sistema general o contra usuarios, proveedores u operadores, contra la autoridad fiscalizadora* (Estado); para todos los casos, las sanciones quedan pendientes a tipificarse en un reglamento posterior.

2.3. Ley Nº 341 "Ley de Participación y Control Social"

Con relación al tema de análisis; en la Ley Nº 341 se hace referencia a lo indispensable de apoyar el control social de la administración pública en la informática –ejercido por la sociedad–. Resaltando la necesidad de coadyuvar con la fiscalización y control en todas las áreas de gestión que hacen a la administración pública –los que mediante reclamos o denuncias podrán afectar favorablemente sobre los aspectos ilícitos relativos a informática–; pudiéndose exigir la restitución o reparación integral de la vulneración de un derecho si esto se da, y si constituye un delito, remitirse al ministerio público para ser investigado.

Asimismo, en la Ley Nº 341 se encomienda al Estado la creación de: redes de información, un gobierno electrónico, telecentros y otros instrumentos similares que permitan el control social; incluso se menciona la difusión de informes utilizando sitios web oficiales –aspecto que guarda relación con el Programa Nacional de Telecomunicación de Inclusión Social PRONTIS (D.S. Nº 1391), y con el Gobierno Electrónico (D.S. Nº 1793), ambos a revisarse más adelante.

2.4. Decreto Supremo N° 27330 "Simplificación de Trámites en la Administración Publica"

Aunque de forma indirecta, en el D.S. Nº 27330 se plantea simplificar los procesos de trámites ordinarios recurrentes a los ciudadanos en la administración pública, fin que conlleva apoyarse en la tecnología informática. Sin lugar a duda, pese a que es una importante medida de eficiencia, abre mayores posibilidades para que los ciber delincuentes puedan resultar una nueva amenaza para la sociedad.

2.5. Decreto Supremo Nº 1391 "Reglamento a la Ley Nº 164"

Toda Ley se operativiza mediante reglamentos, como es el caso del D.S. Nº 1391 que complementa la Ley Nº 164. En esta disposición –que corresponde a un Reglamento General–, se regulan y reglamentan todos los aspectos y ámbitos de aplicación de las

actividades de telecomunicaciones y TIC que comprende la Ley antes mencionada. No obstante, respecto a la seguridad informática se reconocen los derechos jurídicos de los usuarios informáticos. También se hacen definiciones similares –y repetitivas– a las encontradas en la Ley Nº 164, entre las que tampoco existe alguna concreta que toque la delincuencia informática.

En esta disposición se considera la interferencia perjudicial como una afectación informática, mencionándose que en ese caso la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transporte (ATT), debe tomar las acciones legales pertinentes. Asimismo, se establece la protección de las operadoras telefónicas en caso de detección de indicios suficientes de fraude o conexiones ilegales, para lo cual el asunto adoptaría una figura legal.

También se abordan algunos inconvenientes posibles a sufrir los usuarios –que pueden dar pautas de delito respecto a uso telefónico y de internet–, para los que la medida de protección es la firma de contratos específicos (relación contractual) con los operadores –abordado desde la perspectiva de protección al consumidor, no contra amenazas o delitos informáticos–.

Adicionalmente, en este Decreto Supremo se menciona sobre la inviolabilidad de datos e información personal y de comunicación de las personas –asequible solo por orden judicial–; mostrándose como delitos: *suplantación de identidad, sustracción, interceptación, interferencia, obstrucción, cambio o alteración de contenidos, desvío de curso de comunicación, publicación, divulgación, diseminación, utilización de contenidos de comunicación*; mismos que, aunque están referidos a telecomunicación, son inferibles a la informática. Sin embargo, se hace evidente un contenido normativo fuertemente proteccionista con relación al Estado, pero no así sobre los usuarios, quienes son los más vulnerables.

2.6. Decreto Supremo Nº 1793 "Reglamento para el Acceso, uso y Desarrollo de las Tecnológicas de Información y Comunicación"

Corresponde a un Reglamento Específico de la Ley Nº 164 referido a software libre, en el que, entre algunas de sus definiciones de importancia para circunscribir un delito informático, ya se identifican dos principales entendimientos importantes para este artículo:

- Seguridad informática, entendida como el *conjunto de normas, procedimientos y herramientas, las cuales se enfocan en la protección de la infraestructura computacional y todo lo relacionada con esta, y especialmente, la información contenida o circulante*.
- Seguridad de la información, definida como la *preservación de la confidencialidad, integridad y disponibilidad de la información; además también pueden estar*

involucradas otras propiedades como la autenticidad, responsabilidad, no repudio y confiabilidad.

Con similar valor, en esta disposición se recomienda el trabajo informático con software libre, que ayudaría a fortalecer la seguridad informática en el país; ámbito de actuación que será supervisado por el Comité Plurinacional de Tecnologías de Información y Comunicación (COPLUTIC).

Por otra parte, en este cuerpo normativo se proponen líneas de acción y políticas de seguridad informática; la creación del Consejo Sectorial de Telecomunicaciones y Tecnologías de Información y Comunicación (COSTETIC), como instancia que trabaje y amplíe más reglamentos –posibilitando los relacionados con la delincuencia informática–.

Por último, además de recalcar sobre la protección de los datos personales; en el D.S. Nº 1793 también se dan varias pautas sobre propiedad y derechos de software libre mediante los certificados digitales, aspecto que constituye un aporte más en términos de seguridad informática.

2.7. Ley Nº 650 "Agenda Patriótica"

Corresponde a otra disposición indirectamente relacionada con el tema del presente artículo; pero útil, puesto que mediante ésta solamente se eleva al rango de Ley la Agenda Patriótica 2025, misma que contiene 13 pilares de trabajo para la realidad boliviana. Siendo que en el pilar 9 (Soberanía científica y tecnológica con identidad propia), se identifica la implicancia de un venidero proteccionismo informático de los usuarios; el que puede concretarse con un marco de reglamentos específicos más nutridos y referidos a seguridad y delincuencia informática.

2.8. Decreto Supremo Nº 2514 "Creación de la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación"

En el D.S. que dispone la creación de la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación, también se inscriben las funciones y atribuciones que este ente tendría, entre las que es bueno mencionar el *establecimiento de lineamientos técnicos de seguridad de información para las entidades del sector público*.

Por otro lado, en esta disposición también se dispone la existencia del Centro de Gestión de Incidentes Informáticos, instancia que serviría para elaborar planes institucionales de seguridad informática. La desventaja es que todo refleja una direccionalidad de beneficio unidireccional para el Estado y no así para los ciudadanos usuarios.

2.9. Ley Nº 777 "Ley del Sistema de Planificación Integral del Estado SPIE"

La Ley Nº 777 –relacionada también de manera indirecta con el tema–, aborda como esencia jurídica el Sistema de Planificación Integral del Estado (SPIE), en el que se integran

todos los procesos de planificación que se dan en el país, entre los que se incorpora el tecnológico informático.

Corresponde a otra forma de ver la toma de decisiones, concibiéndose una nueva forma de planificar el Estado denominado *Planificación Territorial de Desarrollo Integral*, en la que ya se considera la tecnología como parte de la vida ciudadana.

2.10. Ley Nº 779 "Desburocratización para la creación funcionamiento de Unidades Económicas"

De la misma manera, la condicionante de la Ley Nº 779 respecto a la seguridad informática, está en el permitir la creación de mecanismos en calidad de plataformas para mantener controladas todas las Unidades Económicas en el país –personales y jurídicas–; aspecto de relevante relación porque los mecanismos a los que hace referencia son informáticos y de trasfondo económico, lo que implica posibilidades de surgimiento de amenazas informáticas, y por lo tanto ciber delincuencia.

2.11. Decreto Supremo Nº 0667 "Código de Procedimiento Penal"

Finalmente, cabe referirse al D.S. Nº 0667, el que, a pesar que corresponder a todos los delitos penales en general, en dos de sus artículos hace referencia a delitos informáticos.

- Artículo 363 Bis. Manipulación Informática: *el que con la intención de obtener beneficio indebido para sí o un tercero, manipule un procedimiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de tercero, será sancionado con reclusión de uno (1) a cinco (5) años y con multa de sesenta (60) a doscientos (200) días)*
- Artículo 363 Ter. Alteración, Acceso y Uso indebido de Datos Personales: *el que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un (1) año o multa hasta doscientos (200) días)*.

3. Avance en la delincuencia informática y su repercusión en el país

La tecnología informática avanza a pasos gigantescos, y detrás, muy de cerca se pueden identificar cada vez más y nuevas formas de amenazas y de ciber delincuencia; motivo por el cual una buena parte de los avances al respecto se destinan a la creación de medidas correctivas a las vulnerabilidades.

No obstante, las sociedades, aunque son dinámicas, no avanzan al mismo ritmo que lo hace la tecnología informático, por lo que siempre presentara un grado de vulnerabilidad ante los delincuentes informáticos. La distancia entre la consolidación de una nueva

tecnología y la superación de sus amenazas, es lo suficientemente amplia como para que las medidas de contingencias no sean infalibles.

El efecto se hace mayor si las sociedades presentan una fuerte brecha digital –como en el caso de Bolivia–, situación que desemboca en escenarios de alta vulnerabilidad frente a ataques y delincuencia informática. Siendo que la única forma de sobrellevar el retraso digital en este tipo de realidades es disponiendo de un marco jurídico normativo informático bien sólido.

La mayoría de los usuarios –migrantes digitales y nativos digitales inexpertos– no están preparados para muchos aspectos de vida relacionados con la tecnología informática: cuentas bancarias, uso de cajeros automáticos, realización de transacciones en la administración publica, suscripciones, etc., y el acompañamiento legislativo informática tampoco lo está. Dando a entender que es urgente la actuación respecto a la dotación de un marco jurídico normativo en el país, ya que por el otro lado –sensibilización y concientización– implica una tarea de mayor plazo.

4. Implicancias respecto al desbalance entre la evolución del marco legislativo y el crecimiento de la ciber-delincuencia en Bolivia

Pueden surgir varias formas de intervención institucional para remediar los desbalances que se suscitan entre la evolución de la tecnología informática junto a la ciber delincuencia, y el aprendizaje digital ciudadano que permita no ser vulnerable ante las amenazas. Sin embargo, es necesario disponer de un Código Penal Informático que aborde cada uno de los aspectos referidos a los delitos físicos y tangibles ordinarios, pero en su vertiente digital.

El análisis jurídico normativo penal para la ciber delincuencia puede ser una complementación al D.S. Nº 0667, o quizás constituir una disposición diferenciada en el país –eso debe dejarse a cargo de los expertos en el tema legal–; pero debe ser una medida pronta a afrontarse y asumirse.

En toda la normativa analizada se evidencia más resguardo y protección legal para el Estado, en cambio para los usuarios esta previsión es casi nula. Todas las disposiciones referenciadas y observadas desde la seguridad informática, claramente dejan percibir que la sociedad boliviana está expuesta. Es cierto que muchos países también lo están, pero otros a la vez están muy preparados; realidades institucionales y normativas que pueden servir de base para la elaboración de un cuerpo legal que responda a la vulnerabilidad boliviana, y fortalezca el avance con relación al resguardo informático del Estado que ya se tiene.

Bibliografía

Andrade, A. (2013). Ataques informáticos contra entidades financieras. Nuevatel PCS Bolivia S.A.

Consejo para las Tecnologías de Información y Comunicación del Estado Plurinacional de Bolivia CTIC – EPB (2016). Normativa relacionada con las Tecnológicas de Información y Comunicación. Recuperado de: https://www.ctic.gob.bo/normativa-relacionada/

Estado Plurinacional de Bolivia (2011). Reglamento General a la Ley Nº 164 del 8 de agosto de 2011 General de Telecomunicaciones, Tecnologías de Información y Comunicación para el Sector de telecomunicaciones. Recuperado de: https://www.oopp.gob.bo/uploads/DS_1391_REGLAMENTO_A_LEY_164_-_SECTOR_TELECOMUNICACIONES.pdf

Estado Plurinacional de Bolivia (2010). Código Penal y Código de Procedimiento Penal. Ministerio de Justicia, Dirección General de Asuntos Jurídicos. Recuperado de: http://www.justicia.gob.bo/index.php/normativa/informacion-estadistica/doc_download/97-codigo-penal-y-codigo-de-procedimiento-penal-

Estado Plurinacional de Bolivia (2011). Decreto Supremo Nº 1391. Recuperado de: https://www.oopp.gob.bo/uploads/DS_1391_ANEXO_A_DS_1391_-_SECTOR_TELECOMUNICACIONES.pdf

Estado Plurinacional de Bolivia (2011). Ley Nº 164 Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación. Recuperado de: https://www.abe.bo/Descargas/Ley164Telecomunicaciones.pdf

Estado Plurinacional de Bolivia (2011). Reglamento General a la Ley Nº 164 del 8 de agosto de 2011 General de Telecomunicaciones, Tecnologías de Información y Comunicación para el Sector de telecomunicaciones. Recuperado de: http://www.obapyme.org/obapyme_contenido/html/files/Reglamento%20de%20TIC%20V1_0%2018-01-12%20-%20Reglamento%20de%20TIC's%20ok.pdf