UNIVERSIDAD DE CHILE

Facultad de Derecho

Centro de Estudios en Derecho Informático

LA OBLIGACIÓN DEL ESTADO DE MANTENER SOFTWARE SEGURO EN EL GOBIERNO ELECTRÓNICO COMO MANIFESTACIÓN DE SU NORMATIVA Y EN ESPECIAL DE LOS PRINCIPIOS DE EFICIENCIA Y EFICACIA ADMINISTRATIVA.

Memoria de Prueba para optar al grado de Licenciado en Ciencias Jurídicas y Sociales.

AUTOR

Felipe Daniel Báez Robledo

PROFESOR GUÍA: Abogado Sra. Lorena Donoso Abarca

Santiago, Chile

2008

A Agustín.

A Marta y Daniel.

AGRADECIMIENTOS

A Agustín Báez Reyes; Alfredo Real Almendra; Carmen Gloria Briceño Concha; Daniel Báez Cortéz; Daniela Báez Ibarra; Jorge Navarro Suazo; José Tomás Alfonso Cea; Margarita Concha Véliz; Lorena Donoso Abarca; María Francisca Reyes Briceño; Marta Robledo Conejeros; Paola Báez Ibarra; Pilar Reyes Saldías; Raúl Donckaster Fernández; Sergio Truffello Morchio; y a todos quienes cooperaron con este trabajo.

TABLA DE CONTENIDOS.

CAPÍTULO IV

CAPÍTULO V

INTRODUCCIÓN.

El desarrollo del denominado Gobierno Electrónico, Gobierno Digital o E-Government, ha significado una fluidez nunca antes vista en la comunicación entre los particulares y la Administración y entre la Administración misma, a través de computadores equipados con diversos software que permiten, entre muchas otras cosas, el traspaso, la oferta y la administración de información relevante en los más disímiles ámbitos.

¿Está obligada la Administración del Estado a mantener software seguro? ¿Que sucedería si alguien lograse vulnerar la seguridad del software del Estado y evitara que los sujetos que tienen derecho a acceder a información ahí contenida lo hagan, o modificara dicha información, la eliminara u obtuviera información confidencial? ¿Debe responder el Estado por los daños que esto produzca? Y de ser así, ¿en que casos? ¿Debe contar el Estado con software seguro a cualquier costo?

El problema es evidente. Por una parte el Estado tiene el deber de garantizar el Bien Común, lo que implica proveer de aplicaciones eficientes y eficaces, sobre todo en el marco del Gobierno Electrónico, y por otra, debe invertir sus recursos de manera eficiente, o dicho de otro modo, atendiendo a criterios de eficiencia presupuestaria.

En este contexto, el cuestionamiento está dado por la inversión en seguridad, ya sea por la vía de analizar los paquetes de programas que adquiera el Estado a fin de detectar fallas en este sentido, o por el camino de invertir, el propio Estado, en el desarrollo de productos informáticos que satisfagan estándares de calidad, interoperabilidad y seguridad que provean a las personas el adecuado resguardo de sus derechos y garantías. En este sentido es necesario determinar si las exigencias que los principios y normas que la Constitución, las leyes y las normas técnicas o específicas en esta materia imponen al Estado lo obligan a realizar inversiones en seguridad sobre el software que utiliza en el marco propio de sus labores y cual es ese nivel de seguridad esperado, de manera de establecer qué tipo de eventos generarían

responsabilidad para el Estado, y en consecuencia, dilucidar si al efectuar tanto órganos públicos como privados un análisis o intervención, autorizada o no por la misma Administración, de los software que ella desarrolle o adquiera, se estaría cometiendo una infracción a los contratos de licencia que se han celebrado con los proveedores, o cometiendo un delito informático, aunque dichos actos sólo se efectuaran con la finalidad de aumentar la seguridad de los mismos, detectando y denunciando dichas fallas.

Nuestra principal motivación para realizar este trabajo es que como resultado del desarrollo tecnológico experimentado en las últimas décadas, tanto en Chile como en el resto del mundo, el Gobierno Electrónico ha sido uno de los proyectos en que nuestra Administración del Estado ha puesto mayor énfasis, constituyendo esta nueva institución un avance significativo en el ámbito de la gestión pública. Sin embargo, y cada día con mayor importancia y publicidad, se han producido fuertes críticas con relación a la seguridad del software con que se ha implementado este sistema.

En el entendido de que toda actividad administrativa del Estado debe guiarse por los principios de eficiencia y eficacia, ¿no ayuda una regulación clara y uniforme de los estándares de seguridad del software de Gobierno Electrónico para cumplir con los principios y normas que fundamentan las Administraciones estatales modernas, promoviendo el Bien Común y la seguridad jurídica, permitiendo detectar, denunciar y corregir las fallas del sistema?

Pues bien, por tratarse de un fenómeno que en nuestro país lleva pocos años de desarrollo, casi no se han efectuado estudios que lo aborden desde el punto de vista jurídico, a diferencia de lo que ha ocurrido en otros países donde este tema sí se ha tomado en serio, tanto por parte de las autoridades públicas como por los particulares.

¿Es necesario que se produzca un escándalo de grandes proporciones en el que se dañen bienes jurídicos protegidos de quienes interactúan de forma cotidiana entre sí en los sistemas de Gobierno Electrónico, es decir, los particulares y el Estado mismo, por fallas de seguridad del software que utiliza la Administración del Estado para tomar

en serio este tema?. Aquí radica principalmente la necesidad de tratar esta materia. Es evidente que una regulación adecuada para las acciones que han de desarrollar los agentes del Estado para asegurar la eficiencia y eficacia del software que utilizan es muy necesaria.

La hipótesis sobre la que se desarrollará este trabajo es que al Estado le asiste el deber de mantener software seguro, en primer término, como una manifestación de los principios y preceptos constitucionales y legales de aplicación general que lo guían en su actuar, especialmente en lo que se refiere a sus obligaciones de promover el Bien Común y respetar en toda su actuación los principios de eficiencia y eficacia Administrativa; y en segundo término, por la obligación de respetar las normas técnicas específicas para el ejercicio de potestades públicas mediante Gobierno Electrónico, debiendo proveerse para ello herramientas jurídicas adecuadas para el desempeño de esta labor, que al menos compatibilicen los estatutos jurídico - privados de los titulares de derechos sobre el software utilizado por la Administración y los deberes del Estado. Aquí cobran gran relevancia el Derecho de Autor y el Derecho Penal Informático.

Como consecuencia de lo anterior, debemos analizar la problemática de la seguridad de los sistemas que sustentan el Gobierno Electrónico desde el punto de vista de los principios que informan el Derecho Público, especialmente los principios de eficiencia y eficacia, debiendo estudiar la normativa general y especial aplicable al Gobierno Electrónico, que está conformada por la Constitución Política de la República, las leyes que regulan la Administración del Estado y los Decretos Supremos sobre Gobierno Electrónico, además de referirnos a derechos de la personas que eventualmente podrían verse vulnerados, como la protección de la vida privada y la protección de datos personales; todo con el fin de incentivar y dar inicio a futuras investigaciones jurídicas sobre seguridad de la información y las comunicaciones en el ámbito del Gobierno Electrónico, ya que este tema se proyecta como una de las grandes problemáticas de la Administración del Estado en la denominada era digital o de la información. Este es nuestro objetivo general.

También se pretende establecer el marco jurídico preciso en que se funda la obligación del Estado de mantener software seguro, además de identificar los puntos en que se producen contradicciones entre los derechos de los particulares, de los titulares de derechos sobre el software y los deberes del Estado como garante del Bien Común y ejecutor del Gobierno Electrónico, intentado proponer una interpretación, modificación o creación de reglas y principios que permitan su armonización.

Es importante recalcar aquí que no pretendemos analizar si actualmente en Chile se está actuando eficaz y eficientemente en el entorno digital, sino que más importante aún, pretendemos justificar el porqué debe actuarse así y determinar con más o menos detalle algunas formas por las que el Estado podría optar para hacerlo.

Para poder cumplir con los objetivos que nos hemos propuesto, el análisis debe internarse primeramente en los principios y normas de Derecho Público para justificar la obligación del Estado de dar seguridad a los soportes de Gobierno Electrónico, para lo cual comenzaremos dilucidando qué se entiende por Gobierno y Administración del Estado y trataremos el concepto de Servicio Público, estudiaremos las bases que sustentan la existencia de la Administración del Estado y su finalidad, constituida por la promoción del bien común, y señalaremos los principios que toda actuación administrativa debe respetar.

Luego, nos referiremos a los principios de eficiencia y eficacia administrativa, estableciendo su contenido y relación con los demás principios con reconocimiento constitucional y legal, especialmente con el principio de responsabilidad del Estado, que adquiere relevancia respecto de las posibles contravenciones al contenido de estos principios y a la forma en que se debe reparar el daño que esto produciría a los particulares.

En una segunda parte, determinaremos en que consisten las Tecnologías de Información y Comunicación, señalando su concepto y los elementos principales que las componen, dando una breve descripción de lo que entenderemos por hardware, indispensable para comprender el concepto de software, que analizaremos más

detalladamente, incluyendo algunas clasificaciones pertinentes al tema y estudiando el régimen jurídico que se les ha dado en Chile. Será aquí donde nos referiremos a la seguridad del software con el objeto de obtener un criterio que nos permita establecer qué características se esperan de un software para ser considerado seguro.

En una tercera parte, intentaremos establecer la relación que existe entre las Tecnologías de la Información y Comunicación y la Administración del Estado, investigando los elementos que componen el concepto de Gobierno Electrónico, proponiendo una definición adecuada para él y haciendo referencia a la importancia que tiene que el Estado cuente con software seguro en el marco del Gobierno Electrónico. Además intentaremos establecer las principales funciones públicas que a través de este medio se realizan y describiremos la manera en que los particulares y el Estado se han enfrentado a este tema. Es así como revisaremos, por un lado, algunas críticas que sujetos particulares han hecho a la seguridad del software de Gobierno Electrónico, y por otro lado, indagaremos en la seriedad con que el Estado ha abordado esta materia.

Entendiendo que la legislación ius publicista es la forma más importante de regulación para el Gobierno Electrónico, pues el cumplimiento de su contenido es posible de exigir por los particulares, analizaremos críticamente la normativa específica que respecto del Gobierno Electrónico existe, evidentemente que con un marcado énfasis en aquello que se refiera a seguridad del software. Dicha normativa está constituida principalmente por Decretos del Ministerio Secretaría General de la Presidencia (MINSEGPRES), comenzando nuestra tarea desarrollando un pequeño glosario de términos. Reconociendo que nuestra legislación ha ido avanzando en términos de permitir cada vez más el uso de estas tecnologías, y que mucha de su normativa no se refiere directamente al Gobierno Electrónico pero que de todas formas se torna relevante para él, revisaremos las principales normas jurídicas que indirectamente se refieren a la seguridad del software de Gobierno Electrónico, esto es, la ley que tipifica figuras penales relativas a la informática y la ley de protección de datos de carácter personal, en la medida que sean relevantes para el tema.

Finalmente, intentaremos examinar la eficiencia y eficacia que respecto de la seguridad del software ha tenido el gasto que la Administración del Estado ha hecho en materia de Gobierno Electrónico, y nos referiremos a las formas que tiene el Estado de proveerse de software seguro, revisando también su eficiencia y eficacia, además de la legalidad y las posibles consecuencias que trae la adopción de uno u otro método.

Es indudable que la mayor dificultad que enfrentaremos al abordar esta materia es la falta de información precisa y oportuna y la dispersión de dicha información, especialmente en el ámbito referido a la forma en que la Administración del Estado ha invertido en Tecnologías de la información y Comunicación. Otro factor es la falta de literatura nacional que trate la seguridad del software en el Gobierno Electrónico desde el punto de vista jurídico.

Además, la norma NCh2777, que analizaremos, ha sido incorporada al ordenamiento jurídico chileno por medio del Decreto Supremo Nº 83 de 2004 del Ministerio Secretaría General de la Presidencia, que aprueba norma técnica para los órganos del Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos, el que determina el sentido y las modificaciones pertinentes que deberán entenderse parte de la normativa, remitiéndose expresamente a ella. Sin embargo, la NCh2777 es propiedad intelectual del Instituto Nacional de Normalización, y teniendo en cuenta que ella es parte integrante del ordenamiento jurídico chileno nos parece inaceptable que no se encuentre disponible para los particulares.

Así, este trabajo pretende trazar las líneas generales del problema, buscando que se tome en consideración la seguridad del software como tema de Estado, referido a "toda" la actividad que el Estado realice por medios electrónicos, y no sólo en temas sensibles como los datos de carácter personal, en los que se ha comenzado a tomar conciencia y, lo que es más importante, se ha comenzado a actuar en consecuencia.

CAPÍTULO I.
LA ADMINISTRACIÓN DEL ESTADO.

1.- Gobierno, Administración del Estado y Servicio Público.

La Constitución Política de la República, en su artículo 24 inciso primero señala que "el gobierno y la administración del Estado corresponden al Presidente de la República, quien es el Jefe del Estado". Este es el punto de partida desde el cual deberemos analizar que entenderemos por Gobierno, Administración del Estado y Servicio Público.

No existe en nuestra doctrina un criterio único para entender el significado y contenido de estas tres instituciones, sin embargo, del tenor literal de la norma constitucional, especialmente por la conjunción "y", se desprende que el gobierno y la administración del Estado son dos actividades-funciones distintas, que sin embargo comparten la característica de ser ejercidas por el Presidente de la República.

Como nos señala el profesor Rolando Pantoja Bauzá, refiriéndose a la función de gobierno, "la distinción entre las funciones de gobierno y de administración proviene del Constitucionalismo clásico del 1800... Constituyó la fórmula de otorgar al Jefe del Estado un ámbito de libre decisión paralelo a su poder ejecutivo. Según ella, es una regla esencial de buen gobierno de un país que el Jefe del Estado pueda solucionar eficazmente los problemas internos y externos de la nación mediante el dominio pleno de un campo propio de libre apreciación, de un ámbito discrecional, se decía, no sometido a la ley, sino sólo a las normas de la Constitución, que le permitan afrontar con éxito las complejas contingencias de la conducción del Estado."[1]

De la misma manera, el destacado profesor Alejandro Silva Bascuñán decía "dentro de la función ejecutiva se distinguen dos formas de actividad, el gobierno y la administración."

[1] Rolando Pantoja Bauzá. El Derecho Administrativo. Clasicismo y Modernidad. Santiago de Chile. Ed. Jurídica de Chile. 1994. p. 151.

"En este sentido… el gobierno es la actividad que consiste en expresar y transmitir una voluntad de mando en el cuidado del interés general."

"Pero la tarea de mandar tiene que completarse por medio de la disposición y organización de los funcionarios, llamados a favorecer de algún modo el cumplimiento de la voluntad del gobernante; a través de la reunión y distribución de los elementos materiales y económicos indispensables para el logro de los objetivos propuestos; mediante la realización de actos de diverso tipo e índole, conforme a la naturaleza del fin perseguido; a través del planeamiento y funcionamiento de una infinidad de actividades que se proyectan en pro del bien colectivo…"

"La coordinación, subordinación y distribución de los agentes y el estatuto de la función pública; el establecimiento de los diferentes servicios públicos; los diversos medios técnicos, actos y contratos realizados a nombre del Estado, etc., forman la administración."[2]

Sin embargo, con el desarrollo paulatino de la doctrina y la jurisprudencia administrativa nacional, esta distinción se ha ido diluyendo, siendo prácticamente imposible realizar un paralelo entre ambas actividades donde pueda establecerse con nitidez el contenido de una u otra. Es más, las Constituciones Políticas de 1925 y 1980, no hacen ningún tipo de distinción respecto del régimen para impugnar decisiones de gobierno y administración, asimilándolas, con lo que sepultó la esencia de la distinción, esto es, la inimpugnabilidad de los actos de gobierno.

Notando la inutilidad de la distinción, el profesor Mario Bernaschina González señaló que "no es posible sostener, como lo ha hecho la teoría clásica del órgano supremo, que exista una función gubernativa, porque el gobierno es el conjunto de magistraturas del Estado y no una competencia propia de uno de sus órganos, como es el órgano administrador o ejecutivo, como también se le llama. Por consiguiente, la

[2] Alejandro Silva Bascuñán. Tratado de Derecho Constitucional. Tomo I, Principios. Ed, Jurídica de Chile, 1963. p. 339.

función propia del Presidente de la República es la administrativa."[3] El profesor y ex Presidente de la República don Patricio Aylwin Azócar fue aun más lejos, al apuntar que "concebida como actividad, la gubernativa no constituye una especie jurídicamente diferenciable de las actividades legislativa, administrativa y jurisdiccional. Desde el punto de vista estrictamente jurídico, no hay una categoría de actos gubernativos análoga a las de los actos legislativos, administrativos y jurisdiccionales, susceptibles de distinguirse por su origen, por su forma o contenido. La actividad de gobierno se realiza por las tres funciones del Estado, pero principalmente a través de las funciones legislativa y administrativa. De lo dicho resulta que el distingo entre Gobierno y Administración no es una clasificación jurídica. Es, en cambio, un distingo político."[4]

No obstante todo lo dicho, el artículo 24 de la Constitución Política de la República se refiere expresamente al gobierno, por una parte, y a la administración por otra, por lo que ante una distinción constitucional de las funciones ejercidas por el Presidente de la República, por muy difícil que sea su diferenciación, no cabe otra cosa que estimarlas como distintas. En este sentido el profesor Pantoja señala que "el artículo 24 de la Constitución Política de la República se refiere expresamente a las funciones de gobierno y administración dentro del 'Gobierno', por lo que obliga al profesional del derecho a dar un sentido a la voz gobierno, siguiendo aquella antigua máxima jurídica de que los mandatos de la ley deben interpretarse en aquella dirección en que adquieran sentido, descartando los que muevan a concluir de otra manera. Por eso... puede decirse que el gobierno es una actividad que presenta un doble carácter: por una parte consiste en aquella función que la Constitución Política radica en el Presidente de la República para permitirle la dirección superior de los intereses generales de la nación, junto al Congreso Nacional y la Corte Suprema de Justicia, de modo que son actos de gobierno desde esta perspectiva todos los dictados por el Presidente de la República para mantener las relaciones jurídicas con el Congreso Nacional y demás autoridades superiores que conforman la institucionalidad superior del país, así como los actos de la misma índole relativos a las relaciones entre Estados

[3] Mario Bernaschina González, citado por Rolando Pantoja Bauzá. El Derecho Administrativo. Clasicismo y Modernidad. Santiago de Chile. Ed. Jurídica de Chile. 1994. p. 157.
[4] Patricio Aylwin Azócar, citado por Rolando Pantoja Bauzá. El Derecho Administrativo. Clasicismo y Modernidad. Santiago de Chile. Ed. Jurídica de Chile. 1994. p. 158.

o a la aplicación de la normativa internacional, parecer que se vincula a las opiniones de que sobre esta materia emitieran los señores Bernaschino y Aylwin... y, por otra, surge como aquella actividad encaminada a la conservación del orden público en el interior y a la seguridad exterior de la República, según lo afirmara el legislador de la Ley de Reforma Constitucional de 1991 y de la Ley Orgánica Constitucional de Gobierno y Administración Regional, debiendo precisarse además, que los actos que concretan tanto una cuanto otra actividad se hallan sometidos a la Constitución y las leyes, así como a las normas generales y ordinarias que rigen la dictación, tramitación, vigencia e impugnación de los actos que dictan las autoridades administrativas del Estado."[5]

Así las cosas, la Ley Nº 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado (LOCBGAE), en su artículo 1º establece que el ejercicio del gobierno y la administración por parte del Presidente de la República se hará con la colaboración de los órganos que establezcan la Constitución y la leyes, para en su inciso segundo enumerar las personas y órganos que constituyen la Administración del Estado, a saber:

- Los Ministerios: Según el mandato constitucional, los Ministros de Estado son los colaboradores directos e inmediatos del Presidente de la República en el gobierno y administración del Estado, según lo dispone su artículo 33 inciso primero. En este mismo sentido, el artículo 19 de la LOCBGAE señala que los Ministerios son los órganos superiores de colaboración del Presidente de la República en las funciones de gobierno y administración de sus respectivos sectores, los cuales corresponden a los campos específicos de actividades en que deben ejercer dichas funciones.

- Las Intendencias: El Intendente representa al Presidente de la República en su respectiva región, y ejerce sus funciones de acuerdo a las leyes y a las ordenes e instrucciones del Presidente de la República, como lo establece el artículo 100 de la Constitución Política de la República. Además debe supervigilar, coordinar y

[5] Rolando Pantoja Bauzá. El Derecho Administrativo. Clasicismo y Modernidad. Santiago de Chile. Ed. Jurídica de Chile. 1994. p. 160 y ss.

fiscalizar los servicios públicos de la región, como lo señala el artículo 19 de la LOCBGAE, entre otras funciones.

- Las Gobernaciones: El gobernador provincial, según lo dispone el artículo 105 de la Constitución Política de la República y 41 de la Ley Orgánica Constitucional de Bases Generales de la Administración del Estado, ejerce, de acuerdo a las instrucciones del Intendente, la supervigilancia de los servicios públicos existentes en la provincia.

- Los órganos y servicios públicos creados para el cumplimiento de la función administrativa, incluidos la Contraloría General de la República, el Banco Central, las Fuerzas Armadas y las Fuerzas de Orden y Seguridad Pública, los Gobiernos Regionales, las Municipalidades y las empresas públicas creadas por ley.

En términos muy generales, el artículo 25 de la LOCBGAE caracteriza a los servicios públicos como aquellos órganos encargados de satisfacer necesidades colectivas de manera regular y continua. Intentando una definición, el profesor Enrique Silva Cimma nos hace notar la dificultad de la tarea, al señalar que "hoy en día... se nos hace tarea mucho más difícil la de intentar una definición única de servicio público chileno que pueda abarcar, en sus múltiples aspectos, toda la diversa gama de la iniciativa estatal tendiente a satisfacer necesidades públicas."[6] Sin embargo, existe relativo consenso en la doctrina y la jurisprudencia acerca del criterio que debe utilizarse para definirla: su estructura orgánica. Así, el profesor Pantoja ha dicho que "en Chile, las actividades del Estado han de caracterizarse, ante todo, por el órgano que las realiza; en seguida, por el contenido de la función constitucionalmente prefigurada por la Carta Fundamental para ser ejercida por ese órgano"[7] Más profundamente, el profesor Silva Cimma señala que "analizando el problema que nos inquieta desde un ángulo legalista o positivo, creemos que en Chile el servicio publico ha sido tomado desde un prisma preferente, si bien no exclusivamente, orgánico. Toda

[6] Enrique Silva Cimma. Derecho Administrativo Chileno y Comparado; El Servicio Público. Ed. Jurídica de Chile, 1995. p. 48.
[7] Rolando Pantoja Bauzá. El Derecho Administrativo. Clasicismo y Modernidad. Santiago de Chile. Ed. Jurídica de Chile. 1994. p. 140.

concepción que no tuviera, pues, como base este elemento primordial, rebasaría y escaparía al sentido realista de que ha partido nuestro legislador."

"En efecto, si analizamos en primer lugar algunas disposiciones de nuestra Carta Política Fundamental y otros textos de legislación complementaria, nos parece que aquella ha entendido la expresión 'servicio público' en el sentido de órganos componentes o integrantes de la Administración Pública, es decir, entidades de que el Estado se vale para cumplir su política de satisfacer las necesidades públicas."[8] Así, por la particular función que estos órganos cumplen, son quienes más necesitan tener una comunicación confiable y expedita, entre ellos, con el resto de la orgánica administrativa – gubernamental, y especialmente con los particulares.

2.- Bases de la Administración del Estado.

2.1.- El Bien Común.

Uno de los temas más importantes sobre los que ha discutido la ciencia política y el Derecho Administrativo es el fin del Estado, o en otras palabras, cual es el objetivo que toda la estructura orgánica del Estado está llamada a cumplir, debiendo poner en ello todos sus esfuerzos y recursos. "A través del desarrollo histórico han surgido diversas teorías acerca del fin del Estado. Así, hay teorías que afirman un único fin del Estado, otras asignan a éste diversos fines. Por su parte, algunos sostienen que el Estado carece de fines, o que no es correcto preguntarse por los fines del Estado, por ser aspectos extrajurídicos"[9]

En esta materia nuestra Constitución Política es clara, al establecer en su artículo 1º inciso cuarto, que "el Estado está al servicio de la persona humana y su finalidad es promover el bien común, para lo cual debe contribuir a crear las condiciones sociales que permitan a todos y a cada uno de los integrantes de la comunidad nacional su

[8] Enrique Silva Cimma. Derecho Administrativo Chileno y Comparado; El Servicio Público. Ed. Jurídica de Chile, 1995. p. 48.
[9] Humberto Nogueira A. y Francisco Cumplido C. Derecho Político, Introducción a la Política y Teoría del Estado. Instituto Chileno de Estudios Humanísticos. Santiago, 1987. p. 123.

mayor realización espiritual y material posible, con pleno respeto de los derechos y garantías que esta Constitución establece". De este modo, el Estado de Chile tiene como fin, consagrado en su Constitución Política, el bien común.

Buscando definir el vocablo, el profesor Silva Bascuñan nos dice que "si es 'bien' lo que mueve el deseo de la voluntad en busca de su perfección, 'bien común' será aquel que contribuye a la perfección de todos y que, por tal motivo, ha de buscarse mediante el esfuerzo de todos"[10]

Así, las autoridades y órganos que ejercen las funciones de gobierno y administración del Estado, deben desarrollarlas en beneficio de todos. Entendiendo que la comunidad política es una necesidad natural del hombre, condición de su conservación, desenvolvimiento, y plenitud, el fin de esa convivencia política no puede ser otro que prestar las condiciones necesarias para que esa naturaleza humana se conserve, desenvuelva y alcance su plenitud.

Así, los elementos que constituyen la noción de bien común podrían sintetizarse en los siguientes:

- Tiene como base la dignidad de la persona humana, por lo tanto, el bien común comprende el mayor bienestar y realización de las personas sin exclusiones, "el bien común no es una cuestión de número, si se reconoce que todos los hombres tienen una misma dignidad y una naturaleza común, es necesario admitir también que las medidas que se adopten de acuerdo con su naturaleza debe beneficiar no sólo a un grupo o a la mitad más uno de los miembros de la comunidad, sino a todos y a cada uno de ellos."[11]

[10] Alejandro Silva Bascuñán. Tratado de Derecho Constitucional. Tomo I, Principios. Ed, Jurídica de Chile, 1963. p. 124.
[11] Humberto Nogueira A.; Francisco Cumplido C. Derecho Político, Introducción a la Política y Teoría del Estado. Instituto Chileno de Estudios Humanísticos. Santiago, 1987. p. 129.

Al referirse a este tema, el profesor Silva Bascuñan es más directo, al señalar que "el hombre no está autorizado, ni siquiera so pretexto de contribuir al bien general, a sacrificar nada de lo que se refiere a su dignidad."[12]

Este elemento se encuentra expresamente consagrado en el artículo 1º de nuestra Constitución Política de la República.

- El bien común comprende los derechos que garantiza, o sea, no se puede decir que un Estado está encaminando sus acciones hacia su fin, el bien común, si no respeta los derechos que garantiza en su Carta Política Fundamental en virtud de la dignidad de los integrantes de la comunidad. "El bien común, por preeminente que sea, debe su preeminencia al hecho de que no sólo expresa, exterioriza o concreta, sino que garantiza verdaderamente los derechos fundamentales de la persona, y se mantiene, por tanto, como interior a éstos"[13]

- Sin embargo, el bien común no se confunde ni comprende al bien individual, aunque son interdependientes.

Así, el bien común no puede ser caracterizado como la suma de los bienes individuales, pues, algunos miembros de la comunidad podrían considerar como su mayor realización material y espiritual posible, la utilización de ciertos medios para la consecución de ciertos fines a los que la comunidad no adhiere, o incluso rechaza.

Por otra parte, claro está que no puede existir contradicción entre el bien común y el bien individual, sino más bien, como lo explica el profesor Silva Bascuñán "debe observarse que aquél [el bien común] no puede llegar hasta el punto de tomar a su cargo la gestión del bien de cada persona o grupo, sustituyéndose a la

[12] Alejandro Silva Bascuñán. Tratado de Derecho Constitucional. Tomo I, Principios. Ed, Jurídica de Chile, 1963. p. 126.
[13] Jean-Yves Calvez y Jaques Perrin, citado por Humberto Nogueira A.; Francisco Cumplido C. Derecho Político, Introducción a la Política y Teoría del Estado. Instituto Chileno de Estudios Humanísticos. Santiago, 1987. p. 127.

acción y esfuerzo de estos, sino que simplemente permitir y estimular sus iniciativas a fin de que se apliquen con mayor energía a sus especiales propósitos para su particular beneficio y consiguiente progreso colectivo."[14] Aquella es la relación existente entre bien común y bien individual, el primero debe facilitar la consecución del segundo.

- También es indispensable señalar que la obtención del bien común requiere de orden, el que en la sociedad moderna se encuentra dado por el derecho, así, "el bien común es fin cuyo logro requiere orden precisamente porque... es indispensable promover y coordinar esfuerzos, herir intereses, refrenar apetitos, escoger los objetivos que reclama la necesidad y progreso de los componentes y encauzar hacia ellos la acción colectiva."

  "El bien común ha de obtenerse en la justicia, tanto conmutativa en el régimen de las relaciones intersubjetivas, como social para imponer sacrificios en aras de la utilidad general, y distributiva, en fin, con el afán de dar a cada sector lo que corresponda en los medios que dispone la colectividad"[15]

Para concluir, debemos señalar que, como se desprende de los elementos recién mencionados, determinar cual es en la práctica el bien que debe inspirar a un Estado en un momento determinado, habrá que atender a las circunstancias en que este se encuentre, y a la apreciación que de él hagan los miembros de aquella comunidad. "Es posible, y a cada instante la realidad lo confirma, que dentro de la sociedad surjan diversas ideas de bien común, diferentes inspiraciones que configuren otras tantas bases organizativas adecuadas a las metas concebidas, cada una a su turno inspirando sus propias reglas directivas."[16]

---

[14] Alejandro Silva Bascuñán. Tratado de Derecho Constitucional. Tomo I, Principios. Ed, Jurídica de Chile, 1963. p. 126.
[15] Alejandro Silva Bascuñán. Tratado de Derecho Constitucional. Tomo I, Principios. Ed, Jurídica de Chile, 1963. p. 127.
[16] Alejandro Silva Bascuñán. Tratado de Derecho Constitucional. Tomo I, Principios. Ed, Jurídica de Chile, 1963.p. 127.

2.2.- Principios a los que debe observancia la Administración del Estado.

El artículo 3° de la LOCBGAE, señala los principios a los que debe ceñirse toda la actividad de los órganos de la administración del Estado, que según lo que dispone el artículo 7° de la Constitución Política de la República, es aquella actividad realizada en el ámbito de su competencia y en ejercicio de sus potestades. Ahora bien, según lo ya expuesto, la Administración del Estado está constituida por los Ministerios, las Intendencias, las Gobernaciones y los servicios públicos creados para el cumplimiento de la función administrativa, incluidos la Contraloría General de la República, el Banco Central, las Fuerzas Armadas y las Fuerzas de Orden y Seguridad Pública, los Gobiernos Regionales, las Municipalidades y las empresas públicas creadas por ley.

De este modo, y de manera meramente enunciativa, diremos que los principios rectores de la actividad pública de los órganos de la administración del Estado que esta ley establece son:

- Principio de responsabilidad;
- Principios de eficiencia y eficacia;
- Principio de unidad administrativa;
- Principio de oficialidad;
- Principio de impugnabilidad de los actos administrativos;
- Principio de control;
- Principio de probidad y
- Principio de transparencia.

Teniendo en cuenta que este trabajo se focaliza en los principios de eficiencia y eficacia administrativa, haremos una descripción y análisis de ellos, y dilucidaremos su relación con otros principios de derecho público. Además, debido a que estos principios no son mera literatura, sino que constituyen directrices obligatorias para la Administración del Estado, trataremos también, someramente, la responsabilidad del Estado, a través de la cual estos principios pueden hacerse exigibles por los particulares y cobrar vida.

3.- Los Principios de eficiencia y eficacia.

El término eficacia ha sido definido por la Real Academia Española como la "capacidad de lograr el efecto que se desea o se espera". Así, la eficacia se relaciona con el logro intencionado, en tanto orientado a un fin predeterminado, de un resultado o consecuencia determinada por parte de una persona. De este modo, la expresión eficacia se refiere a las acciones que un sujeto realiza con el objetivo de cumplir con ciertas y determinadas metas propuestas, por lo tanto, trata sobre la capacidad de un sujeto para satisfacer una necesidad a través del suministro de bienes o servicios.

La eficiencia, por su parte, es la virtud y facultad para obtener un resultado determinado, centrándose no tanto en el resultado mismo, sino que en la aptitud o capacidad del agente para producirlo. "La eficiencia se vincula a la 'productividad' y atiende fundamentalmente a la consecución del máximo nivel de satisfacción posible a alcanzar con los recursos disponibles."[17] La Real Academia Española la ha definido como la "capacidad de disponer de alguien o de algo para conseguir un efecto determinado"

En otras palabras, mientras la eficacia significa hacer las cosas bien, la eficiencia supone hacer bien las cosas, en tiempo y forma. Por ello, la profesora Gladys Camacho Cepeda asevera que "la eficiencia no se preocupa de los fines, sino de los medios, y por

[17] Claudio Moraga K. Principios con reconocimiento legal a que debe observancia la administración del Estado. Apuntes de clases (primer semestre 2002). p. 4.

su parte, el logro de los objetivos previstos no es competencia de la eficiencia sino de la eficacia."[18]

Íntimamente relacionado con los principios de eficiencia y eficacia se encuentra el principio de economía, el que alude a la adecuada administración financiera de los recursos limitados con los que se cuenta, de manera de intentar que dichos recursos se aprovechen en un cien por ciento, o lo más cercano posible a eso.

De esta manera, los principios de eficiencia y eficacia denotan que la legitimidad de la actuación de los órganos públicos no sólo debe fundamentarse en la legalidad, sino que además en la forma y sentido como la Administración del Estado cumple las tareas públicas y de gobierno, es decir, se espera que el Estado, y particularmente la Administración pública, no sólo resuelva los problemas, sino que lo haga oportunamente y conforme a una racional utilización de los recursos, lo que supone, entre otros, mejorar la gestión pública, fomentar el desarrollo tecnológico, simplificar y dar rapidez a los trámites que ante ellos se realizan, mejorar el aprovechamiento de los medios disponibles, establecer procedimientos administrativos ágiles y expeditos, etcétera.

Según la profesora Camacho "los principios de eficacia y eficiencia administrativas se estatuyen positivamente como deberes de doble concreción: como deber jurídico de la Administración, en cuanto organización sustantivada; y como deber de las autoridades y funcionarios."[19]

La única referencia constitucional al principio de eficiencia se encuentra en su Capítulo XIV, al disponer el artículo 115 inciso tercero, que la distribución de las Inversiones Sectoriales de Asignación Regional (ISAR) se deben hacer de acuerdo a los criterios de equidad y eficiencia. Por su parte, el artículo 14 de la Ley N° 19.175 Orgánica Constitucional sobre Gobierno y Administración Regional, señala los

[18] Gladys Camacho Cepeda, citado por Claudio Moraga K.: Principios con reconocimiento legal a que debe observancia la administración del Estado. Apuntes de clases (primer semestre 2002). p. 4.

[19] Gladys Camacho Cepeda, citado por Claudio Moraga K.: Principios con reconocimiento legal a que debe observancia la administración del Estado. Apuntes de clases (primer semestre 2002). p. 4.

principios a los que deberán sujetarse los Gobiernos Regionales, estableciendo, al lado de la equidad, los principios de eficacia y eficiencia en la asignación y utilización de recursos públicos y en la prestación de servicios.

Así, a primera vista, pareciese que para estimar eficaz y eficiente el cumplimiento de las funciones públicas por parte de los órganos de la Administración del Estado, las herramientas con las que se ejecutan estas tareas también deberán serlo. En el entendido que el software es una herramienta para la ejecución de dichas funciones, éste debe ser también eficaz y eficiente.

3.1.- Ámbitos de operación de los principios de eficiencia y eficacia.

Ahora bien, la norma establecida en el artículo 3° de la LOCBGAE, ya mencionada, debe entenderse referida a los principios de eficiencia y eficacia como deber jurídico de todos los órganos de la Administración del Estado, mientras que el artículo 5° inciso primero de la misma ley debe asociarse con estos principios como deber propio de las autoridades y funcionarios públicos, en cuanto señala que las autoridades y funcionarios deberán velar por la eficiente e idónea administración de los medios públicos y por el debido cumplimiento de la función pública.

Como consecuencia de lo anterior, podemos decir ya con argumentos suficientes, y siguiendo al profesor Claudio Moraga Klenner[20], que la eficiencia y eficacia se encuentran referidas a toda la actuación de la Administración del Estado, incluso a la actuación de sus autoridades y funcionarios, operando entonces en los siguientes ámbitos:

- Ámbito propio de cada actuación administrativa concreta, determinada por un fin específico y cumpliendo con el mandato fundamental del artículo 1° inciso tercero de la Constitución, esto es, orientada a procurar el bien común y encaminada a su efectiva realización;

[20] Ver: Claudio Moraga K.: Principios con reconocimiento legal a que debe observancia la administración del Estado. Apuntes de clases (primer semestre 2002). p. 4.

- Ámbito referido a la actividad de una organización administrativa en su conjunto, cuya función se encuentra delimitada por la suma de las competencias/potestades que le atribuye el ordenamiento jurídico vigente, y para demandar que la misma muestre como resultado el mejor cumplimiento posible de la función que a aquella organización le corresponda desempeñar como parte integrante del sistema administrativo; y

- Ámbito constituido por la actuación global de cada una de estas administraciones públicas (estatal, regionales y comunales), para buscar la más plena realización del bien común a través de dicha actuación administrativa, considerada en su conjunto.

3.2.- Vinculación de los principios de eficiencia y eficacia con otros principios de Derecho Público.

Ahora bien, y siguiendo nuevamente al profesor Moraga, los principios de eficacia y eficiencia tienen su sustento en el principio de responsabilidad, el que será tratado más adelante, sin el cual se tratarían sólo de una manifestación de buenas intenciones. Además, los principios de eficiencia y eficacia "se encuentran vinculados necesariamente con los principios de coordinación, control y probidad,"[21] en los siguientes términos:

- Con el principio de coordinación, puesto que la eficiencia y eficacia suponen necesariamente la existencia de una coordinación administrativa para garantizar la unidad de acción de la Administración y excluir las duplicidades o interferencia de funciones, como está establecido en el artículo 5° inciso segundo de la LOCBGAE.

- Con el principio de control la relación se debe entender en el ámbito del control jerárquico que corresponde a las autoridades administrativas, dentro del ámbito de sus competencias. Esto no sólo se refiere a una Administración que actúe correcta y

[21] Claudio Moraga K.: Principios con reconocimiento legal a que debe observancia la administración del Estado. Apuntes de clases (primer semestre 2002). Pág. 4.

con respeto a las disposiciones legales, sino una Administración que responda con oportunidad al cumplimiento de sus fines para garantizar al ciudadano su derecho al libre desarrollo de su persona. “La misión institucional debe traducirse en metas y objetivos concretos susceptibles de medición o apreciación en cuanto a su logro u obtención (...) A su vez, los medios y recursos con que cuenta la Administración deben ser establecidos con claridad, coherencia y precisión por el Ordenamiento jurídico - público.”[22]

Si fuese de otro modo, no sería posible cumplir el deber establecido legalmente en el artículo 12 de la LOCBGAE, según el cual las autoridades y funcionarios deben velar permanentemente por el cumplimiento de los planes y la aplicación de las normas.

Ahora bien, el artículo 11 inciso segundo del la LOCBGAE, establece positivamente que el control administrativo interno jerárquico no sólo se refiere a la legalidad y oportunidad de las actuaciones de la Administración, sino que le corresponde extenderse a la eficiencia y eficacia en el cumplimiento de los fines y objetivos establecidos. Por su parte, el artículo 52 inciso segundo del D. L. N° 1.263 Orgánico de Administración Financiera del Estado, señala que la verificación y evaluación del cumplimiento de los fines y de la obtención de las metas programadas para los servicios públicos, son funciones que competen primordialmente a la Administración del Estado y cuyo ejercicio corresponde al Poder Ejecutivo y no sólo a los órganos fiscalizadores, como por ejemplo la Contraloría General de la República.

- Respecto del principio de probidad, debe destacarse que la prevalencia del interés general exige el empleo de medios idóneos de diagnóstico, decisión y control, para concretar dentro del orden jurídico, una gestión eficiente y eficaz, tal como lo señala el artículo 53 de la LOCBGAE.

[22] Claudio Moraga K.: Principios con reconocimiento legal a que debe observancia la administración del Estado. Apuntes de clases (primer semestre 2002). Pág. 4.

Si se produjese un incumplimiento de este deber jurídico, este podría ser tipificado como una violación al principio de probidad administrativa, ya que entre las conductas expresamente señaladas como contrarias a este principio por el artículo 62 N° 8 de la LOCBGAE se encuentra la contravención de los deberes de eficiencia y eficacia que rigen el desempeño de la función pública.

3.3.- La especial vinculación con el principio de responsabilidad del Estado.

Podemos decir que este es el principio más importante en lo que se refiere a la actividad de los órganos de la Administración del Estado, ya que sin responsabilidad el resto de los principios y normas que los reconocen no tendrían un sustento donde materializarse, por ello, el reconocimiento de la responsabilidad del Estado establece una garantía de protección a los administrados. Conceptualizando, el profesor Silva Cimma señala que "la responsabilidad es la carga con que se obliga a una persona para que asuma las consecuencias de su conducta y, aún en ciertas circunstancias, por la de terceros o por los hechos de sus cosas."[23]

A nivel constitucional, la responsabilidad del Estado se encuentra regulada principalmente en los artículos 6° [24] inciso final, 7° [25] inciso final, 19 N° 7 letra i)[26], 36[27]

---

[23] Enrique Silva Cimma, citado por Claudio Moraga K.: Principios con reconocimiento legal a que debe observancia la administración del Estado. Apuntes de clases (primer semestre 2002). p. 1.

[24] "Art. 6º. C.P.R. Los órganos del Estado deben someter su acción a la Constitución y a las normas dictadas conforme a ella.

Los preceptos de esta Constitución obligan tanto a los titulares o integrantes de dichos órganos como a toda persona, institución o grupo.

La infracción de esta norma generará las responsabilidades y sanciones que determine la ley"

[25] "Art. 7º. C.P.R. Los órganos del Estado actúan válidamente previa investidura regular de sus integrantes, dentro de su competencia y en la forma que prescriba la ley."

"Ninguna magistratura, ninguna persona ni grupo de personas pueden atribuirse, ni aun a pretexto de circunstancias extraordinarias, otra autoridad o derechos que los que expresamente se les hayan conferido en virtud de la Constitución o las leyes."

"Todo acto en contravención a este artículo es nulo y originará las responsabilidades y sanciones que la ley señale."

[26] "Art. 19. C.P.R. La Constitución asegura a todas las personas:"

"7.º El derecho a la libertad personal y a la seguridad individual."

"En consecuencia:"

"i) Una vez dictado sobreseimiento definitivo o sentencia absolutoria, el que hubiere sido sometido a proceso o condenado en cualquier instancia por resolución que la Corte Suprema

y 38 inciso segundo[28]. Por su parte, a nivel legislativo, la responsabilidad se encuentra consagrada principalmente en los artículos 4 y 42 de la LOCBGAE[29] y en el artículo 141 de la Ley Orgánica Constitucional de Municipalidades[30].

El régimen de responsabilidad del Estado es una de las materias más controvertidas en el ámbito del Derecho Administrativo, existiendo opiniones doctrinarias diversas y muchas veces contrapuestas. Sin embargo, ellas pueden sintetizarse en dos grandes grupos: aquellos que defienden la responsabilidad objetiva del Estado y aquellos que estiman que la responsabilidad del Estado se basa en criterios subjetivos, en este caso, cuando se ha incurrido en falta de servicio. Esta controversia se produce debido a que ni la Constitución ni las leyes explicitan si el Estado debe responder basado en criterios objetivos o subjetivos.

Que en Chile el Estado es responsable por sus actos, y que dicha responsabilidad se basa en la legislación administrativa de Derecho Público es algo que ya se ha reconocido tanto por la doctrina como por la jurisprudencia, descartándose la aplicación del régimen de responsabilidad que establece el Título XXXV del Libro Cuarto del Código Civil, salvo contadísimas excepciones.

---

declare injustificadamente errónea o arbitraria, tendrá derecho a ser indemnizado por el Estado de los perjuicios patrimoniales y morales que haya sufrido. La indemnización será determinada judicialmente en procedimiento breve y sumario y en él la prueba se apreciará en conciencia;"

[27] "Art. 36. C.P.R. Los Ministros serán responsables individualmente de los actos que firmaren y solidariamente de los que suscribieren o acordaren con los otros Ministros"

[28] "Art. 38. inc. 2º C.P.R. Cualquier persona que sea lesionada en sus derechos por la Administración del Estado, de sus organismos o de las municipalidades, podrá reclamar ante los tribunales que determine la ley, sin perjuicio de la responsabilidad que pudiere afectar al funcionario que hubiere causado el daño"

[29] "Artículo 4º.- El Estado será responsable por los daños que causen los órganos de la Administración en el ejercicio de sus funciones, sin perjuicio de las responsabilidades que pudieren afectar al funcionario que los hubiere ocasionado."

"Artículo 42.- Los órganos de la Administración serán responsables del daño que causen por falta de servicio."

"No obstante, el Estado tendrá derecho a repetir en contra del funcionario que hubiere incurrido en falta personal."

[30] "Artículo 141.- Las municipalidades incurrirán en responsabilidad por los daños que causen, la que procederá principalmente por falta de servicio."

"No obstante, las municipalidades tendrán derecho a repetir en contra del funcionario que hubiere incurrido en falta personal."

La doctrina según la cual el Estado responde cuando se ha producido una falta de servicio, liderada por el profesor Pedro Pierry Arrau, se basa principalmente en que el artículo 38 inciso segundo de la Constitución Política del Estado, considerado la piedra fundamental para quienes sostienen que en Chile existe un régimen de responsabilidad objetiva, no sería más que una norma de competencia. Así, "para Pierry, este artículo 38 inciso segundo no es un precepto sustantivo de responsabilidad del Estado sino que es una 'norma de competencia' para determinar el tribunal que debe conocer el contencioso – administrativo y no de una acción de responsabilidad. Según él, así se desprendería claramente de las Actas de Sesiones de la Nueva Constitución... y si con todo, se llegara a sostener que se trata de una acción de responsabilidad, no aparece en absoluto claro que se trate de una responsabilidad objetiva, sino todo lo contrario... De ello infiere Pierry que la responsabilidad del Estado es subjetiva porque 'siempre se consideró que la responsabilidad del Estado únicamente podría verse comprometida en caso de una actuación antijurídica.'"[31] Por falta de servicio debemos entender el hecho de no haberse prestado el servicio debiendo haberse prestado, haberlo prestado mal o en forma tardía.

Por su parte, esta doctrina afirma que el artículo 4º de la LOCBGAE entiende la responsabilidad ligada al actuar ilícito o antijurídico del Estado, por lo tanto, sustentado en dolo o culpa de servicio. Basa su afirmación en el informe de la comisión redactora de dicha ley, el que dice "El artículo 3 (actual 4) del anteproyecto reproduce el principio de responsabilidad del Estado por los daños que los órganos de la Administración produzcan en el ejercicio de sus funciones, sin perjuicio de las responsabilidades que pudieran afectar al funcionario que hubiere causado el daño. En consecuencia, cabe aplicar aquí la regla general sobre indemnización por los daños que cause la Administración debiendo determinarse, en cada caso, por los tribunales competentes, si ella actuó con culpa o dolo"[32]

[31] Fabián Andrés Huepe Artigas. Responsabilidad del Estado, Falta de Servicio y Responsabilidad Objetiva en su Actividad Administrativa. Santiago – Chile. Instituto Chileno de Derecho Administrativo. 2004. p 71.

[32] Citado por Fabián Andrés Huepe Artigas. Responsabilidad del Estado, Falta de Servicio y Responsabilidad Objetiva en su Actividad Administrativa. Santiago – Chile. Instituto Chileno de Derecho Administrativo. 2004. p 71.
p 71.

En efecto, sería el artículo 42 de la LOCBGAE, donde se establecería expresamente la responsabilidad por falta de servicio, lo que trae aparejado un problema adicional, ya que el artículo 21 de la misma ley excluye de la aplicación de su Título II, donde se encuentra el artículo 42, a la Contraloría General de la República, al Banco Central, a las Fuerzas Armadas y de Orden y Seguridad Públicas, a las Municipalidades, al Consejo Nacional de Televisión y a las empresas públicas creadas por ley. Salvo respecto de las Municipalidades, que tienen en el artículo 141 de la Ley Orgánica Constitucional de Municipalidades, una norma particular redactada en los mismos términos que el artículo 42 de la LOCBGAE, Pierry afirma que a estos órganos de la Administración del Estado excluidos de la aplicación del artículo 42, deben aplicárseles las normas de Derecho Común para determinar su responsabilidad, en especial el artículo 2314 del Código Civil.

En la doctrina de la responsabilidad objetiva del Estado, por otra parte, sostenida por los Profesores Soto Kloss, Fiamma, Pantoja, Caldera, entre otros, se reconoce que el principio de responsabilidad tiene un carácter absoluto, esto es, toda actividad, hecho u omisión en el sector público que de lugar a un daño, produce responsabilidad, excepto si el daño se produce como consecuencia de caso fortuito o fuerza mayor.

El fundamento de esta doctrina está en la interpretación armónica de los artículo 6, 7 y 38 inciso segundo de la Constitución Política de la República, entendiendo además que en ninguna de aquellas normas se establece la necesidad de la concurrencia de elementos subjetivos de culpa o dolo de servicio para hacer efectiva la responsabilidad del Estado por los daños producidos en el patrimonio de un particular, sino que bastaría sólo el daño y el nexo causal entre dicho daño y una actividad pública.

En este entendido, las normas de los artículos 4 y 42 de la Ley Orgánica Constitucional de Bases Generales de la Administración del Estado, sólo podrían interpretarse en el mismo sentido que la Constitución da al régimen de responsabilidad del Estado, esto es, como responsabilidad objetiva.

Esta doctrina considera que la Constitución Política de la República establece el principio de responsabilidad de los órganos del Estado por los daños que produzca en

su actividad en contra de una víctima que no se encuentra jurídicamente obligada a soportarlo, por lo tanto, si el daño se produce en el patrimonio de un tercero, debe responder el Estado, pero éste puede repetir contra el funcionario autor del daño; si el daño se causa por el funcionario en la propia Administración, la responsabilidad será personal de aquél, y si el daño es cometido por actos, hechos u omisiones imputables a un particular en perjuicio del Estado, éste debe perseguir las responsabilidades del tercero.

El profesor Pantoja, explicando esta doctrina ha dicho que "en verdad, cabe pensar que el artículo 44 [actual 42] es aplicación de la norma base establecida en el artículo 4º. No sería dable suponer, por una parte, que el legislador ha incorporado una regla de responsabilidad objetiva en una disposición y un precepto diferente en el artículo 44 [actual 42], debiendo existir entre las normas de una ley la debida correspondencia y armonía, y porque aceptar un punto de vista distinto del expresado, significaría, por la otra, afirmar la inconstitucionalidad del artículo 44 [actual 42], corolario que por su gravedad sólo es admisible alcanzar cuando se poseen irredargüibles piezas de convicción que lleven a sostener esa conclusión, lo que no sucede en este caso."

"Por lo mismo, preciso es concluir que los artículos 4º y 44 [actual 42] de la LOCBGAE guardan entre sí la debida correspondencia y armonía, y que la solución de derecho que dan al tema de responsabilidad extracontractual del Estado Administración se basa en la teoría pública objetiva, que se configura por el daño causado por los organismos administrativos con su actuar lícito o ilícito, jurídico o de hecho, sin perjuicio de que tratándose de los órganos y organismos regidos por el 'Título II – Normas Especiales', haya de configurarse por el demandante la falta de servicio que le sirve de causa de pedir.''[33]

De esta manera, la responsabilidad del Estado se puede ver comprometida cualquiera que sea la actividad que desarrolla en el ejercicio de sus diversas funciones,

[33] Rolando Pantoja Bauzá, citado por Fabián Andrés Huepe Artigas. Responsabilidad del Estado, Falta de Servicio y Responsabilidad Objetiva en su Actividad Administrativa. Santiago – Chile. Instituto Chileno de Derecho Administrativo. 2004. p 82.

sin perjuicio de la responsabilidad particular que pudiere alcanzar al funcionario agente de daño. Dicha responsabilidad se asienta, además, en el principio según el cual nadie puede ser privado de lo suyo, es decir, menoscabado en sus situaciones jurídicas subjetivas, o perturbado en sus condiciones normales de existencia, sino en la medida que la propia Constitución haya contemplado esa posibilidad, y en las condiciones que ella ha arbitrado al efecto.

El artículo 6° de la Constitución Política de la República establece que la infracción a la obligación de los órganos del Estado de someter su actuación a la Constitución y a las normas dictadas conforma a ellas generará las responsabilidades y sanciones que determine la ley.

En el entendido que la obligación del Estado de actuar con respeto a los principios de eficiencia y eficacia está establecida en una ley dictada conforme a la Constitución, su actuación ineficaz e ineficiente que produzca daño en el patrimonio de un tercero genera la obligación de responder. Si se adhiere a la teoría de la responsabilidad objetiva, no cabría duda que, salvo caso fortuito o fuerza mayor, el Estado debe responder, sin perjuicio de la posibilidad de repetir contra el funcionario; y si, por su parte, se adhiere a la teoría de la responsabilidad por falta de servicio, los daños que se produzcan en circunstancias de desoírse los principios de eficiencia y eficacia configuran claramente una falta de servicio.

CAPÍTULO II
LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

1.- Concepto de Tecnologías de la Información y Comunicación.

Intentar dar un concepto de Tecnologías de la Información y Comunicación (TIC) no es una tarea fácil, ya que se trata de un término difuso que se utiliza frecuentemente para designar una variedad de elementos que se refieren principalmente a la informática y a sus aspectos sociales. Sin embargo, es necesario introducirnos en él, ya que éste es el punto de partida desde el cual se desarrolla la íntima relación entre el software y los órganos de la Administración del Estado, que da nacimiento al Gobierno Electrónico. Por esto, aunque de forma somera, es necesario intentar establecer sus elementos más relevantes.

Así, por TIC podemos entender al conjunto de elementos que permiten la administración de información, especialmente, pero no exclusivamente, referida a los ordenadores o computadores en su aspecto físico y al software, indispensable para convertirla, administrarla, almacenarla, encontrarla y transmitirla. La utilización masiva de estas tecnologías ha producido el desarrollado del concepto de Sociedad de la Información. "Los primeros pasos hacia una Sociedad de la Información se remontan a la invención del telégrafo eléctrico, pasando posteriormente por el teléfono fijo, de la radiotelefonía y, por último, de la televisión. Internet, la telecomunicación móvil y el GPS pueden considerarse como nuevas TIC."[34]

Se habla de Sociedad de la Información para referirse al profundo cambio que se ha producido con el progresivo avance del uso de las TIC en las sociedades actuales; de esta manera, el concepto de TIC no sólo se refiere al conjunto de innovaciones tecnológicas que permiten un mejor y más fluido intercambio, almacenamiento y

[34] Fundación Iberoamericana para la Gestión de la Calidad (FUNDIBEQ). Boletín Electrónico Aprender de los Mejores – Octubre Nº 5 [en línea] <http://www.iberpymeonline.org/Documentos/AprenderMejores5.pdf> [consulta: 23 de agosto de 2007]

administración de información, sino que también a la aptitud que tienen estas herramientas para producir una redefinición radical del funcionamiento social, influyendo su aplicación práctica en los más disímiles ámbitos de las actividades humanas, pero sin duda uno de los mejores ejemplos de su influencia sobre la sociedad es el Gobierno Electrónico.

Debemos decir que uno de los efectos al que los investigadores actuales han prestado mayor atención es que el acceso desigual a los progresos que aportan las TIC ha producido una nueva forma de exclusión social, que se ha denominado Brecha Digital.

Así, las nuevas TIC, operan de una manera compleja, requiriendo de un sustento para su desarrollo e implementación, el que está dado principalmente por el hardware y el software.

La Real Academia Española define hardware como un vocablo inglés que se refiere al "conjunto de los componentes que integran la parte material de una computadora." y es el término técnico que se utiliza para referirse a "los componentes físicos, dispositivos de estado sólido y similares, de un sistema informático"[35], siendo ejemplos de ello, el monitor, el teclado, la impresora, etcétera. La Unidad Central de Proceso (CPU) es el hardware que contiene los elementos necesarios para almacenar el software, y es a través de él que se administra la relación con los periféricos, que como es evidente, también son hardware.

Las TIC primitivas, como el teléfono análogo, funcionaban prácticamente sólo en base a lo que hoy denominamos hardware, ya que se trataba de circuitos que permitían el envío de información, en este caso sonidos codificados en impulsos eléctricos, los que se traspasaban por medio de cables hasta otros circuitos, que los decodificaban para que el receptor pudiera comprenderla. Por su parte el receptor sólo podía acceder a ella en el momento en que la comunicación se producía, ya que no

[35] Otto Colomina Pardo, Francisco Flores R., Jerónimo Mora P. Introducción a la Informática para Juristas. Alicante. Ed. Club Universitario. 1997. p. 17.

existía, primeramente, la opción de almacenarla, convertirla ni administrarla. Como se observa, dichas tecnologías funcionaban en base a efectos físicos básicos y naturales, sin la necesidad de realizar tareas como las que desarrolla la disciplina denominada programación, que tuvo un surgimiento posterior.

De esta forma, las Nuevas TIC no operan por sí solas; el soporte material y los fenómenos físicos básicos no son suficientes para caracterizarlas, requiriendo algo más, que les permita interrelacionarse de una forma más compleja, eficiente y eficaz, siendo este elemento el software. En otras palabras, un entramado de materiales como latas, cables, etcétera, que no obstante son elementos esenciales para el concepto actual de TIC, no funcionan sólo por efectos físicos básicos, sino que requieren de intervención especializada para obtener los resultados que hoy conocemos, tales como comunicación instantánea, interoperabilidad, almacenamiento de información, etcétera, y esa intervención está dada por el software.

2.- El software.

2.1.- Concepto.

El término software ha sido definido por la Real Academia Española como “conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora.”

El software está compuesto por los programas que permiten el funcionamiento del computador, siendo información codificada que se transmite al hardware, para que este la procese y ejecute; en otras palabras, “es información que se almacena en la memoria, y no permanece en los circuitos, por lo que no puede ser modificado fácilmente para adaptarse a los requerimientos de los usuarios, sirviendo de enlace entre máquina y usuario.”[36]

[36] Otto Colomina Pardo, Francisco Flores R., Jerónimo Mora P. Introducción a la Informática para Juristas. Alicante. Ed. Club Universitario. 1997. p. 17.

En el plano netamente jurídico, la definición de software en nuestro país está dada por el artículo 5° letra t) de la ley N° 17.336 sobre propiedad intelectual, que lo caracteriza como "conjunto de instrucciones para ser usadas directa o indirectamente en un computador a fin de efectuar u obtener un determinado proceso o resultado, contenidas en un cassette, diskette, cinta magnética u otro soporte material." En este mismo sentido, se ha señalado que software o programa computacional es el "conjunto de instrucciones expresadas mediante palabras, códigos, planes o en cualquier otra forma que, al ser incorporadas en un dispositivo de lectura automatizada y traducidas en impulsos electrónicos, pueden hacer que un computador – aparato electrónico similar apto para elaborar informaciones – ejecute determinada tarea u obtenga determinado resultado."[37]

El lenguaje utilizado por el software para comunicarse con el hardware es de tipo binario, el cual sólo es ocupado por sistemas electrónicos o tecnológicos. Pero finalmente todo este lenguaje viene en forma de instrucciones, las cuales son ejecutadas por cada una de las partes del hardware.

Como ejemplos de software podríamos señalar un sistema operativo, un procesador de texto, una hoja de cálculo, un juego, etcétera.

El hardware y el software son los elementos que definen la naturaleza de un sistema informático actual, siendo ambos conceptos complementarios, ya que a través del software cualquier usuario tiene la posibilidad de traspasar a un computador sus necesidades. Esta tarea es desarrollada por las denominadas aplicaciones de software, que simulan y extienden algunas propiedades de elementos comunes de la vida, como un lápiz, un pincel, una hoja, un archivador, una máquina de escribir, etcétera, "permitiendo hacer con los computadores cosas que, sin ellos, resultarían

[37] Felipe Schuster Pineda. Programas de Computación/software [en línea] <http://www.universidadvirtual.cl/downloads/laadaptacion.ppt> [consulta: 20 de abril de 2006]

tediosas y muy difíciles."[38] Esto trae como consecuencia la obtención de resultados más rápidos, eficientes y eficaces.

Sin embargo, los sistemas informáticos requieren además de un elemento que sirva para enlazar las aplicaciones y el hardware, lo que es realizado por el sistema operativo, "el cual hace transparente al usuario la utilización eficiente de los recursos mecánicos y electrónicos del sistema."[39]

De esta forma, el software permite, por una parte, que las personas internen en el computador un sinnúmero de problemas y, por otra, que estos les provean respuestas y soluciones.

2.2.- Clasificación.

Como ya esbozáramos, el software admite clasificación, para lo cual utilizaremos dos criterios. El primero se referirá al ámbito en que el software sea útil, mientras el segundo atenderá a las formas en que se distribuye o comercializa el software.

2.2.1.- Según ámbito de utilidad.

2.2.1.1.- Software de sistema.

Este tipo de software es el encargado de controlar todo el sistema, permitiendo que el proceso de comunicación con el hardware sea más sencillo y que funcione de una manera eficiente. Todo computador depende de los denominados sistemas operativos. "En esencia, el sistema operativo aísla al usuario de tener que controlar cada dispositivo y cada bit que se introduce en la máquina."[40]

---

[38] Otto Colomina Pardo, Francisco Flores R., Jerónimo Mora P. Introducción a la Informática para Juristas. Alicante. Ed. Club Universitario. 1997. p. 18.
[39] Otto Colomina Pardo, Francisco Flores R., Jerónimo Mora P. Introducción a la Informática para Juristas. Alicante. Ed. Club Universitario. 1997. p. 18.
[40] Otto Colomina Pardo, Francisco Flores R., Jerónimo Mora P. Introducción a la Informática para Juristas. Alicante. Ed. Club Universitario. 1997.p. 40.

Brevemente, las tareas fundamentales del software de sistema son las siguientes:

- Comunicarse con los periféricos: El software de sistema es el encargado de controlar el flujo de información entre la Unidad Central de Procesos y el monitor, el teclado, la impresora, etcétera

- Coordinar el procesamiento de las tareas: Se encarga de optimizar el trabajo del sistema, evitando los posibles intervalos inactivos y aprovechando al máximo los recursos disponibles. Esto lo realiza repartiendo los tiempos de procesamiento que se da a cada tarea del sistema informático.

- Administrar la memoria: Este software se encarga del procesamiento de distintos requerimientos en un mismo instante. El sistema operativo debe controlar la forma en que se utiliza la memoria, de manera que las tareas no se obstaculicen entre sí.

- Administrar los programas y datos: Es el sistema operativo quien permite al usuario del computador la localización o acceso a los programas o datos que éste requiere.

Finalmente, podemos señalar que los sistemas operativos también pueden clasificarse atendiendo a su capacidad para realizar sus tareas en ordenadores personales, en superordenadores o en ambos.

2.2.1.2.- Software de aplicaciones.

Software de aplicaciones, o aplicaciones, son aquellos programas de computador que permiten al ordenador realizar tareas específicas, como escribir un texto, hacer cálculos, navegar por Internet o simplemente jugar. Una característica llamativa de este tipo de software es que muchas veces se aplica sólo en ámbitos de interés muy especializados, careciendo de relevancia para quienes no se desarrollan en aquellos campos específicos de actividades.

Como ejemplos de algunos ámbitos de interés en los que se utilizan este tipo de software podemos señalar:

- Procesamiento de textos y publicaciones electrónicas: El procesamiento de texto es una herramienta fundamental para cualquier persona o institución que requiera comunicarse por escrito, tanto en papel como en forma digital, ya que permite la utilización de un sinnúmero de estilos o tipos de letras, tamaños y diseños. Además, la mayoría de ellos actualmente permiten una corrección automática de ortografía y gramática en el idioma que el operador requiera.

- Hojas de cálculo y otras aplicaciones de cálculo numérico: Las aplicaciones de cálculo permiten la realización de operaciones matemáticas complejas de forma más sencilla, además de permitir tablas numéricas, estudios estadísticos, etcétera, pudiendo relacionarlos a través de fórmulas predeterminadas que el usuario sólo debe ingresar en el computador, dando un resultado exacto.

- Bases de datos para almacenamiento y recuperación de información: Este tipo de software permite almacenar, administrar y recuperar todo tipo de información de una manera más eficiente y eficaz, evitando la utilización de grandes espacios físicos y ahorrando el tiempo que se necesitaría para su recuperación.

- Redes y telecomunicaciones: El intercambio de información y la comunicación entre computadores ubicados en los puntos más lejanos unos de otros requiere de software de aplicación desarrollados para esto. A través de estas aplicaciones se puede acceder a cualquier otra aplicación, de cualquier tipo, que se encuentre disponible en una red determinada.

- Diseño gráfico para ordenadores: Los computadores además de trabajar con texto y números permiten el desarrollo de todo tipo de dibujos, gráficos, diseños, planos, animaciones bidimensionales y tridimensionales, etcétera.

- Multimedia: Las aplicaciones multimedia permiten la combinación de audio, video y texto, lo que permite la transferencia de información de una manera más atractiva, amigable y entretenida.

- Inteligencia artificial: El desarrollo de la tecnología ha permitido la utilización de computadores en áreas específicas otorgándoles facultades que tradicionalmente se han atribuido sólo al ser humano. Un ejemplo de ellos es el reconocimiento de caracteres manuscritos, eliminación de defectos en imágenes, etcétera

No obstante la clasificación, no taxonómica, de los ámbitos de interés en que pueden desarrollarse los software de aplicaciones, la mayoría de este tipo de software, actualmente combinan dos o más de estos ámbitos de interés, haciéndolos más sencillos y eficientes en la satisfacción de las necesidades de los usuarios.

2.2.1.3.- Software de desarrollo.

Se entiende por software de desarrollo aquel que se utiliza para crear otro software, lo que se logra dándole instrucciones mediante un computador que lo posee, instrucciones que este tipo de software puede entender y procesar, dando como resultado un nuevo software.

Como ya dijéramos, los computadores poseen su propio lenguaje, llamado binario, esto es, unos y ceros, y es a través de éste que los software de desarrollo pueden procesar las instrucciones. Los programadores actuales utilizan lenguajes de alto nivel y muy complejos, que se encuentran en una posición intermedia entre los lenguajes específicos de los computadores y los lenguajes naturales humanos. “Estos lenguajes permiten que los científicos e ingenieros resuelvan problemas utilizando una terminología y una notación familiares, en lugar de oscuras instrucciones de máquina”[41]. Es a estos lenguajes de programación que se les denomina software de desarrollo.

[41] Otto Colomina Pardo, Francisco Flores R., Jerónimo Mora P. Introducción a la Informática para Juristas. Alicante. Ed. Club Universitario. 1997. p. 43.

La especificidad del conocimiento necesario para la adecuada utilización de este tipo de software ha permitido el nacimiento de una disciplina profesional, la programación.

2.2.2.- Según su Forma de Comercialización o Distribución.

2.2.2.1.- Software libre.

"Es aquel software que puede ser distribuido, modificado, copiado y utilizado libremente por quien lo use, por lo tanto, debe estar disponible su código fuente para hacer efectivas las libertades que lo caracterizan. Dentro del concepto de software libre hay, a su vez, matices que es necesario tener en cuenta. Por ejemplo, software de dominio público es aquel que no está protegido por el copyright, por lo tanto, podrían generarse versiones no libres del mismo, en cambio el software libre protegido con copyleft impide a los redistribuidores incluir algún tipo de restricción a las libertades propias del software así concebido, es decir, garantiza que las modificaciones hechas en él seguirán siendo software libre."[42] También es conveniente no confundir el software libre con el software gratuito, ya que el hecho de que su costo de adquisición sea cero no lo convierte en software libre, ya que este concepto no se relaciona con su precio, sino que con las libertades que el usuario puede ejercer sobre él.

2.2.2.2.- Software propietario.

El concepto de este tipo de software es residual, entendiéndose por tal aquel que "no es libre, y por lo tanto, su distribución, redistribución, modificación y copia están prohibidas o, al menos, tan restringidas que es imposible hacerlas efectivas." [43]

---

[42] José J. Grimaldos Parra. Manual Básico de Uso Guadalinex Edu [En línea] <http://www.juntadeandalucia.es/averroes/manuales/guadaconceptos.html> [Consulta: 16 de octubre de 2006]

[43] José J. Grimaldos Parra. Manual Básico de Uso Guadalinex Edu [En línea] <http://www.juntadeandalucia.es/averroes/manuales/guadaconceptos.html> [Consulta: 16 de octubre de 2006]

Como aparece evidente, el concepto de código fuente es básico para entender la diferencia entre software propietario y software libre, y puede definirse como el "conjunto de instrucciones que componen un programa informático"[44]

2.2.2.3.- Freeware.

No existe una definición clara y precisa de este tipo de software, sin embargo podemos decir que, en general, se refiere al "software que puede redistribuirse libremente, pero no modificarse, ya que no está disponible su código fuente." [45] Por lo tanto, no debe confundirse con el software libre.

2.2.2.4.- Shareware.

"Es un software que permite su redistribución, sin embargo no se encuentra disponible para el usuario su código fuente, y por tanto, no puede ser modificado. Además, pasado un periodo de tiempo, normalmente es necesario pagar una licencia para continuar usándolo." [46] Así, es una especie de software propietario de prueba, en el que luego de pasado un tiempo, el usuario deberá decidir si lo adquiere o no.

2.3.- Régimen jurídico del software en Chile.

Como se observó al clasificar el software según su forma de comercialización o distribución, el software puede protegerse jurídicamente, lo que en cada país está dado por la concepción que de éste se tenga.

---

[44] Definición.org. Definición de Código Fuente [en línea] <http://www.definicion.org/codigo-fuente> [consulta: 30 de abril de 2006]
[45] José J. Grimaldos Parra. Manual Básico de Uso Guadalinex Edu [En línea] <http://www.juntadeandalucia.es/averroes/manuales/guadaconceptos.html> [Consulta: 16 de octubre de 2006]
[46] José J. Grimaldos Parra. Manual Básico de Uso Guadalinex Edu [En línea] <http://www.juntadeandalucia.es/averroes/manuales/guadaconceptos.html> [Consulta: 16 de octubre de 2006]

Desde su surgimiento, las legislaciones de los distintos países comenzaron a darle protección mediante su agregación al catálogo de obras protegidas por medio del Derecho de Autor, siendo Filipinas el primero en hacerlo en el año 1972. En 1980 Estados Unidos siguió la misma tendencia. “En otros países se consideran protegidos por derecho de autor sin necesidad de una reforma legislativa pues la enumeración de las obras no está sujeta a numerus clausus.”[47]

El Convenio de Berna para la Protección de las Obras Literarias y Artísticas del 9 de septiembre de 1886, vigente en Chile desde el 10 de julio de 1975, en su artículo 2° establece la protección de las obras literarias y artísticas, señalando que estas “comprenden todas las producciones en el campo literario, científico y artístico, cualquiera que sea el modo o forma de expresión, tales como los libros, folletos y otros escritos; las conferencias, alocuciones, sermones y otras obras de la misma naturaleza; las obras dramáticas o dramático-musicales; las obras coreográficas y las pantomimas; las composiciones musicales con o sin letra; las obras cinematográficas, a las cuales se asimilan las obras expresadas por procedimiento análogo a la cinematografía; las obras de dibujo, pintura, arquitectura, escultura, grabado, litografía; las obras fotográficas a las cuales se asimilan las expresadas por procedimiento análogo a la fotografía; las obras de artes aplicadas; las ilustraciones, mapas, planos, croquis y obras plásticas relativos a la geografía, a la topografía, a la arquitectura o a las ciencias.”

Aunque el artículo trascrito no se refiere expresamente a los programas de computador, debe entenderse que ellos pueden encuadrarse dentro de las obras protegidas en el mismo régimen dado a las obras literarias, ya que como dijimos, estos se expresan a través de lenguajes, denominados lenguaje de programación o código fuente y código objeto. El código fuente es aquel “creado por el ser con semántica propia y una sintaxis, como cualquier lengua idiomática”[48] mientras que el código

[47] Felipe Schuster Pineda. Programas de Computación/software [en línea] <http://www.universidadvirtual.cl/downloads/laadaptacion.ppt> [consulta: 20 de abril de 2006]
[48] Felipe Schuster Pineda. Programas de Computación/software [en línea] <http://www.universidadvirtual.cl/downloads/laadaptacion.ppt> [consulta: 20 de abril de 2006]

objeto es “otra forma de lenguaje, que traduce el programa fuente a unos signos que pueden ser leídos por el computador mediante un programa compilador.”[49]

En este mismo sentido, el Tratado OMPI (Organización Mundial de la Propiedad Intelectual) sobre Derecho de Autor (TODA), del que nuestro país es parte y que tiene como objeto mejorar la protección a algunas obras, entre las cuales se encuentran los programas de computador, señala en su artículo 2° que “la protección del derecho de autor abarcará las expresiones pero no las ideas, procedimientos, métodos de operación o conceptos matemáticos en sí.” De esta manera, respecto de la protección de los programas de computador podemos decir, desde ya, que el objeto de dicha protección no es ni el método ni el procedimiento, sino que “la forma de expresión cualquiera que sea, por lo que debe entenderse tanto al código objeto como al código fuente.”[50]

Como confirmación de los recién expuesto, el TODA, en su artículo 4°, establece que “los programas de ordenador están protegidos como obras literarias en el marco de lo dispuesto en el Artículo 2° del Convenio de Berna. Dicha protección se aplica a los programas de ordenador, cualquiera que sea su modo o forma de expresión.”

Por su parte, el artículo 3° número 16 de la ley sobre propiedad intelectual, establece de manera expresa la protección legal de la propiedad intelectual sobre los programas computacionales, cualquiera sea el modo o forma de expresión, como programa fuente o programa objeto, por lo tanto, la protección se otorga cualquiera sea el soporte en que tales programas se encuentren contenidos.”

Respecto del momento en comienza la protección del software, el artículo primero de la ley sobre propiedad intelectual señala claramente que la protección de cualquier obra, incluidos los programas de computador, comienza en el momento de su creación y por ese sólo hecho, y por lo tanto, desde ese instante el Derecho de Autor, otorga a

[49] Felipe Schuster Pineda. Programas de Computación/software [en línea] <http://www.universidadvirtual.cl/downloads/laadaptacion.ppt> [consulta: 20 de abril de 2006]
[50] Felipe Schuster Pineda. Programas de Computación/software [en línea] <http://www.universidadvirtual.cl/downloads/laadaptacion.ppt> [consulta: 20 de abril de 2006]

su titular una serie de derechos, que se clasifican en derechos morales y derechos patrimoniales, permaneciendo la protección legal de la obra, en general, por toda la vida de su autor y se extiende por el plazo de hasta setenta años más, contados desde el fallecimiento del autor, en el caso que sea persona natural, y cincuenta años a contar desde la primera publicación en el caso de ser el autor una persona jurídica, tal como lo establece el artículo 10 de la ley sobre propiedad intelectual, perteneciendo luego la obra al patrimonio cultural común.

Ahora bien, los derechos morales pueden ser ejercidos sólo por el autor de la obra, si aún viviese, y son transmisibles únicamente por causa de muerte a su cónyuge y herederos abintestato, siendo inalienables y nulo todo pacto en contrario a estas disposiciones, tal como lo señalan los artículos 14, 15 y 16 de la ley sobre propiedad intelectual, y son:

- Derecho de Paternidad: Derecho a reivindicar la paternidad de la obra, asociando a la misma el nombre o seudónimo conocido del autor (Artículo 14 N° 1 de la ley sobre propiedad intelectual).

- Derecho de Integridad: Derecho del autor a oponerse a toda deformación, mutilación, u otra modificación hecha a la obra sin su expreso y previo consentimiento. (Artículo 14 N° 2 de la ley sobre propiedad intelectual).

- Derecho de Divulgación: Derecho del autor a mantener su obra inédita (Artículo 14 N° 3 de la ley sobre propiedad intelectual).

- Derecho de Terminación: Derecho del autor para autorizar a terceros a terminar la obra inconclusa, previo consentimiento del editor o cesionario si los hubiere (Artículo 14 N° 4 de la ley sobre propiedad intelectual).

- Derecho de Anonimato: Derecho del autor a exigir que se respete su voluntad de mantener la obra anónima o seudónima mientras esta no pertenezca al patrimonio cultural común (Artículo 14 N° 5 de la ley sobre propiedad intelectual).

Por su parte, los derechos patrimoniales o de explotación dan derecho a su titular para beneficiarse económicamente de su producción intelectual y pueden ser enajenados a terceros distintos del autor. En todo caso pueden ejercerse también por quienes estuvieren expresamente autorizados por el titular e incluso pueden renunciarse. Estos derechos son:

- Derecho de Publicación: Derecho a utilizar la obra publicándola mediante su edición, grabación, emisión radiofónica o de televisión, representación, ejecución, lectura, recitación, exhibición y, en general, cualquier otro medio de comunicación al público, actualmente conocido o que se conozca en el futuro (Artículo18 letra a) de la ley sobre propiedad intelectual).

- Derecho de Reproducción: El titular de este derecho patrimonial puede obtener beneficio económico de las reproducciones que se realicen de la obra o recurso por cualquier procedimiento. (Artículo 18 letra b) de la ley sobre propiedad intelectual).

- Derecho de Transformación: Derecho para recibir ganancias por la adaptación de la obra a otro género, o la utilización en cualquier otra forma que entrañe una variación, adaptación o transformación de la obra originaria, incluida la traducción (Artículo 18 letra c) de la ley sobre propiedad intelectual).

- Derecho de Ejecución Pública: Se entiende como ejecución pública de la obra su emisión por radio o televisión, discos fonográficos, películas cinematográficas, cintas magnetofónicas u otro soporte material apto para ser utilizado en aparatos reproductores de sonidos y voces, con o sin imágenes, o por cualquier otro medio (Artículo 18 letra d) de la ley sobre propiedad intelectual).

En este entendido, ante la pregunta sobre quién es el titular del Derecho de Autor sobre el software, el artículo 8° incisos segundo y tercero de la ley sobre propiedad intelectual establece que “tratándose de programas computacionales, serán titulares del derecho de autor respectivo las personas naturales o jurídicas cuyos dependientes,

en el desempeño de sus funciones laborales, los hubiesen producido, salvo estipulación escrita en contrario“ y “respecto de los programas computacionales producidos por encargo de un tercero para ser comercializados por su cuenta y riesgo, se reputarán cedidos a éste los derechos de su autor, salvo estipulación escrita en contrario.”

En efecto, nuestra ley sobre propiedad intelectual señala expresamente quién será el titular del Derecho de Autor sobre software en estos dos casos especiales: la creación de software por encargo y la creación de software por personas bajo subordinación y dependencia en el ejercicio de sus funciones, aplicándose para el resto de los casos las normas generales para determinar la autoría o coautoría de las obras, como sería el caso de una persona natural que con sus propios medios y conocimientos desarrolle un software, o el caso en que un grupo de personas entre las cuales no existe vínculos de dependencia ni subordinación realicen aquella tarea. La norma general en esta materia se encuentra en el artículo 8° inciso primero de la ley sobre propiedad intelectual, que establece que “se presume que es autor de la obra la persona que figure como tal en el ejemplar que se registra, o aquella a quien, según la respectiva inscripción, pertenezca el seudónimo con que la obra es dada a la publicidad.” Sin embargo, el artículo 15 número 1 del Convenio de Berna para la Protección de las Obras Literarias y Artísticas establece que “para que los autores de las obras literarias y artísticas protegidas por el presente Convenio sean, salvo prueba en contrario, considerados como tales y admitidos, en consecuencia, ante los tribunales de los países de la Unión para demandar a los defraudadores, bastará que su nombre aparezca estampado en la obra en la forma usual. El presente párrafo se aplicará también cuando ese nombre sea seudónimo que por lo conocido no deje la menor duda sobre la identidad del autor.” Queda claro que la ley chilena y el Convenio de Berna tienen diferentes criterios en esta materia; por una parte, la ley sobre propiedad intelectual hace descansar la presunción de autoría en el registro de la obra en el Conservador de Propiedad Intelectual, mientras que el Convenio de Berna presume autor a quien aparezca como tal en la forma usual, pero en todo caso, ambas normas establecen una presunción simplemente legal, la que puede ser desechada si se produce plena prueba en contrario.

El fundamento de esta afirmación se encuentra en el artículo primero de la ley sobre propiedad intelectual, donde se establece que la protección comienza en el momento y por el sólo hecho de la creación de la obra, y por lo tanto, el trámite de inscripción en el Registro de Propiedad Intelectual tiene como una de sus consecuencia que se presuma como autor a quien figure en él, pero si un tercero logra probar fehacientemente que es el autor y no quien figura en el registro, debe reconocérsele a él como autor, y en consecuencia, resarcírsele de todos los perjuicios que el impostor le hubiere causado.

2.4.- Seguridad del Software.

Habiendo establecido el régimen jurídico del software en Chile, corresponde ahora descifrar qué es o qué características tiene un software seguro, pero intentar determinar dichas características o requerimientos no es una tarea sencilla, ya que como veremos, de acuerdo con las principales funciones públicas que pueden desarrollarse a través del Gobierno Electrónico, un software que sea considerado seguro en este ámbito deberá contar con una serie de características interrelacionadas.

1. La primera de ellas es que el software esté en condiciones de continuar con un funcionamiento correcto ante cualquier ataque que intente alterarlo. Evidentemente nos referimos a ataques que se puedan llevar a cabo por medio de TIC, ya que el software también puede ser atacado de otras formas, como la intervención directa de una persona en el ordenador en que se sostiene el software, o casos fortuitos, como incendios, etcétera, que son materia de la seguridad de los aspectos físicos de la informática.

2. Íntimamente relacionada con la anterior, una segunda característica del software seguro es que la información que se almacene en ellos, y los canales de comunicación para enviar o recibir información, se encuentren siempre disponibles para los usuarios.

3. Respecto al acceso a la información que por este medio se maneja, es también muy importante que el software sea capaz de dar acceso a ella sólo a las personas que estén autorizadas para obtenerla, contando con mecanismos que permitan la autenticación de los usuarios, esto es, la confirmación de la identidad del usuario y que dicho sistema también sea seguro.

4. La cuarta característica es que el software sea capaz de custodiar y proteger los datos que maneja, esto es, los datos que almacena, recibe y entrega, ante cualquier manipulación no autorizada que intente conocerlos, modificarlos o eliminarlos, sea de forma consciente o inconsciente.

De este modo, y siguiendo al profesor Pablo García Pérez, podemos decir que software seguro es aquel que "sigue funcionando correctamente frente a cualquier ataque, que da acceso a la información que utiliza sólo a usuarios autorizados (autenticándolos cuando sea necesario), que custodia los datos que maneja y los protege frente a manipulación consciente o inconsciente de los usuarios y que su disponibilidad esté garantizada."[51]

El uso indebido de las redes informáticas afectan tanto a la seguridad de los sistemas como a la integridad y validez de la información que en ella se contiene o que a través de ella se transfiere, y las redes que soportan el Gobierno Electrónico son susceptibles de ataques y operaciones no autorizadas debido a que se encuentran dispersas geográficamente y que son múltiples los equipos y sistemas que forman parte de ellas.

El hecho de ser las redes y el software inseguros ante determinados ataques "puede dar lugar a que ciertos derechos y libertades de que gozan los ciudadanos en

[51] Pablo García Pérez. Principios Básicos de Desarrollo Seguro [en línea] <http://www.germinus.com/sala_prensa/articulos/ppos%20basicos%20desarrollo%20seguro.pdf > [consulta: 23 de marzo de 2006]

otros ámbitos de la comunicación convencional no puedan ser ejercidos eficazmente en entornos de Comunicaciones Mediante Computadores (CMC)"[52]

La inseguridad del software no se refiere sólo a ataques premeditados y conscientes en contra de ellos, sino que también a ataques involuntarios o inconscientes de los propios usuarios.

Así, un documento soportado electrónicamente se puede modificar o falsificar, por lo que, en este sentido, no presentaría ninguna ventaja respecto de un documento escrito en papel. Además, en el caso de los documentos electrónicos sería más sencillo hacerse pasar por otra persona, ya que no es necesaria la comunicación presencial, sustituyéndose por un acceso remoto. Todo esto produce que la información que se transfiere o se almacena electrónicamente sea poco fiable; ello hace que, "admitiendo este tipo de limitaciones, sea inviable hablar de cualquier proyección digital de escenarios de comunicación que en la actualidad se llevan a cabo usando, por ejemplo, el papel como soporte."[53] Sin embargo, ya existen programas y mecanismos que hacen este tipo de comunicación más confiable y segura.

No obstante, en la actualidad, la vulneración de la seguridad del software que soportan los sistemas informáticos es uno de los principales incentivos para los intrusos. Así por ejemplo, las páginas Web, donde se pone a disposición del público gran cantidad de información relevante, son la imagen pública de las instituciones, de manera que vulnerarlas, modificarlas o evitar su disponibilidad podría significar una importante pérdida en imagen y credibilidad de dicha institución, lo que acarreará graves perjuicios en el ámbito de la Administración pública, y además, pérdida de clientes en el caso de las empresas privadas. De esta forma, la explotación de fallas de

[52] Justo A. Carracedo Gallardo: *Provisión de protocolos de anonimato para la protección de la privacidad y el desarrollo de la democracia electrónica en las comunicaciones mediante computadores,* En: Heriberto Cairo Carou (Ed) Democracia Digital, Limitaciones y Oportunidades. p. 31.
[53] Justo A. Carracedo Gallardo: *Provisión de protocolos de anonimato para la protección de la privacidad y el desarrollo de la democracia electrónica en las comunicaciones mediante computadores,* En: Heriberto Cairo Carou (Ed) Democracia Digital, Limitaciones y Oportunidades. p. 31.

seguridad del software de instituciones importantes, es planteada como un desafío para los intrusos, y su consecución motivo de satisfacción personal.

CAPÍTULO III.
EL GOBIERNO ELECTRÓNICO COMO UTILIZACIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN EN LA ADMINISTRACIÓN DEL ESTADO.

1.-Tecnologías de la Información y Comunicación en la Administración del Estado.

El significativo desarrollo que ha tenido en los últimos años el uso de las TIC ha provocado un fuerte impacto en los distintos ámbitos del quehacer de las sociedades y de la actividad económica, pues entre otras cosas, ha facilitado que se realicen distintos tipos de actividades y procesos de la vida cotidiana de un modo más eficaz y eficiente.

A lo largo del desarrollo histórico de los diversos ámbitos del Derecho Público comparado y nacional, pueden identificarse un sinnúmero de hechos y fenómenos de gran relevancia, pero sin duda, ninguno de ellos planteó mayores desafíos para las Administraciones públicas, los administrados y el derecho, como los que hoy plantea el uso de TIC en la ejecución de funciones públicas. A partir de este fenómeno, se ha producido un cambio fundamental en la forma en que la Administración proporciona información y se prestan los servicios públicos, desarrollándose un concepto que sugiere un proceso cuyo objetivo es una forma de gobierno que implica algo muy cercano a una revolución, una redefinición de los marcos espaciales, temporales y de relaciones que permite efectivamente hablar con propiedad de una nueva forma de Administración del Estado, distinta a las formas que la han antecedido.

Resulta prácticamente indiscutible considerar que el Estado tiene un rol fundamental en los procesos de cambio de un país, liderándolos y transformándose en una especie de usuario modelo, actuando como un agente catalizador para la sociedad, que está atenta a sus experiencias.

Según la Agenda Digital Chile 2004-2006, “las Tecnologías de la Información y Comunicación no son un fin en sí mismas. Son instrumentos para modernizar el Estado, incrementar la productividad y acortar las diferencias entre grandes y pequeñas empresas, mejorar la eficiencia de las políticas sociales, disminuir las disparidades regionales de desarrollo y aumentar la equidad.”[54]

En la mayoría de los países del mundo la mayor organización proveedora y recolectora de información es el Estado, la mayoría de los servicios que brinda son monopólicos y sus actuaciones son esencialmente públicas, como emitir certificados de nacimiento, defunción y matrimonio, realizar certificaciones o fiscalizaciones laborales, educacionales y ambientales, entre otros. El profesor Silva Cimma ha dicho que “en todo Estado políticamente organizado existirán ciertos cometidos que el Estado habrá de satisfacer por intermedio de sus propios órganos que integran la Administración. Son los cometidos esenciales, que desde las primeras épocas en la evolución del Derecho Público el Estado ha debido atribuirse para sí: la defensa nacional, la justicia, la fiscalización, son cometidos que sólo al Estado corresponde cumplir. No sin cierta razón se les ha denominado ‘servicios públicos de monopolio’ porque la actividad que el Estado desarrolla para obtenerlos en miras siempre a lograr el fin último, cual es el bienestar de la colectividad, sólo corresponde a los órganos de la Administración” [55]

Al tener la Administración del Estado un monopolio sobre dichas materias, los usuarios de los servicios ofrecidos por ella están cautivos, siéndoles imposible realizar una selección de oferta o de proveedores. Por ejemplo, nadie puede solicitar los certificados de nacimiento, defunción o matrimonio en otro organismo que no sea aquel que la ley señala como oficial. Del mismo modo, tampoco se pueden exigir plazos o condiciones distintas a las establecidas en la legislación. Como consecuencia de este monopolio, podría pensarse que no existen incentivos naturales para la implementación de procesos y estrategias innovadoras en pos de mejorar la calidad del servicio entregado y satisfacer las expectativas de los usuarios.

[54] Grupo de Acción Digital. Agenda Digital Chile 2004-2006. p.5
[55] Enrique Silva Cimma. Derecho Administrativo Chileno y Comparado; El Servicio Público. Ed. Jurídica de Chile, 1995. p. 16.

Sin embargo, el auge que ha tenido la utilización de TIC en el ámbito público implica precisamente hacer un esfuerzo por mejorar los servicios entregados a los particulares, pero este esfuerzo no se basa en criterios de racionalidad económica fundamentados en la idea de competencia dentro de un mercado, sino que más bien por razones jurídico - políticas.

Incentivar la participación ciudadana, proveer de información oportuna y veraz a la ciudadanía, facilitar el acceso de los particulares a los servicios públicos y a una comunicación continua y expedita con la Administración, y entre la Administración misma, son elementos que se consideran esenciales en una democracia moderna, que de no promoverse podrían producir críticas de parte de la ciudadanía y de los adversarios políticos. Ahora bien, en el mundo actual se encuentran disponibles para las Administraciones Públicas una gran gama de TIC, que precisamente son herramientas fundamentales para obtener como resultado aquello que las sociedades democráticas actuales exigen, y por otro lado, es la misma existencia de las TIC lo que hace a las sociedades exigirlo. Es en este círculo donde se encuentra el incentivo para la utilización de TIC por parte de la Administración del Estado.

De esta forma, existiendo, por una parte, las herramientas y los medios para proveer los elementos antes citados, que sirven tanto para lograr niveles de eficiencia y eficacia nunca antes vistos en el ejercicio de las actividades públicas como para mejorar sustancialmente el funcionamiento de la Administración; y por otro lado, teniendo en cuenta la obligación del Estado de promover el bien común, puede decirse que los incentivos señalados se encuentran también consagrados en nuestro ordenamiento jurídico, tanto en la Constitución Política de la República como en las leyes que regulan los órganos de la Administración del Estado, especialmente en lo que dicen relación con los principios de eficiencia y eficacia en la actividad de las reparticiones públicas.

Sin embargo, los incentivos políticos y legales que han dado pie al desarrollo del Gobierno Electrónico no han sido suficientes, especialmente en lo referido al acceso

igualitario de los particulares a esta nueva forma de relación con la Administración del Estado, como también respecto de la seguridad de los software que se utilizan para su sustento. Es especialmente en este último punto donde cobra especial relevancia la falta de incentivos naturales para mejorar la calidad del servicio entregado. Esto se debe a tres elementos íntimamente relacionados. En primer lugar, la novedad que actualmente representa el uso de este tipo de tecnologías en las relaciones entre el Estado y los particulares trae como consecuencia que gran parte de los usuarios potenciales de ellas no posean los conocimientos específicos requeridos para evaluar la calidad del servicio prestado; en segundo lugar, el ya mencionado monopolio del Estado en la prestación de muchos de aquellos servicios desemboca en que no exista la necesidad de cautivar a los usuarios por medio de un servicio de calidad; y en tercer lugar, la desconfianza que existe en la ciudadanía respecto de la seguridad de los sistemas informáticos, manifestada por el temor de muchos particulares a ser víctima de fraudes o delitos, o a que se utilicen sus datos personales de forma inadecuada.

Así, algunos aspectos esenciales para una adecuada relación entre las TIC y el Estado no son objeto de interés primordial de la Administración del Estado, y uno de los elementos que no se han considerado en nuestro país con carácter prioritario es precisamente la seguridad del software del Gobierno Electrónico. Sin embargo, las críticas sobre los elementos técnicos relacionados con él ya se han comenzado a desarrollar, aunque a cargo de expertos en la materia.

2.- Concepto de Gobierno Electrónico.

Dado que el alcance de este fenómeno aún es muy difícil de dimensionar, no existe un concepto único de lo que debe entenderse por Gobierno Electrónico o E-government. Los distintos esfuerzos en este sentido intentan identificar aquellas actividades públicas realizadas o apoyadas a través del uso de TIC.

Procederemos a revisar algunos de los conceptos que se han desarrollado para esta actividad.

El ex Presidente de la República, don Ricardo Lagos Escobar, en el Instructivo Presidencial de Gobierno Electrónico, de 11 de mayo de 2001, señaló que el término Gobierno Electrónico debe entenderse como "el uso de las NTIC (Nuevas Tecnologías de la Información y Comunicación) para mejorar los servicios e información ofrecidos a los ciudadanos, aumentar la eficiencia de la gestión pública e incrementar sustantivamente la transparencia del sector público y la participación ciudadana."[56]

Ahora bien, según un estudio realizado conjuntamente por el Proyecto de Reforma y Modernización del Estado del Ministerio Secretaría General de la Presidencia y el Programa de Modernización de la Gestión Pública del Departamento de Ingeniería Industrial de la Facultad de Ciencias Físicas y Matemáticas de la Universidad de Chile, el Gobierno Electrónico consiste en "facilitar el acceso, mediante el uso de tecnologías de información y comunicaciones, de los ciudadanos, organizaciones y gobierno a información, servicios y/o diálogo con la Administración pública, a todos los niveles jerárquicos, organizacionales y territoriales."[57]

Por su parte, el Servicio de Impuestos Internos (S. I. I.), uno de los organismos públicos cuyas aplicaciones de Gobierno Electrónico tienen mayor relevancia social, al permitir a los contribuyentes declarar su impuesto a la renta, emitir facturas y boletas de honorarios y realizar los trámites de inicio de actividades, entre otros, todo por vía electrónica, entre otras, ha establecido que "el Gobierno Electrónico (e-government) es un concepto de gestión que fusiona el empleo intensivo de Tecnologías de la Información y Comunicación (TIC), con modalidades de gestión y administración, como una nueva forma de Gobierno. En el caso de Chile, este concepto fue elevado a política de Estado."[58]

---

[56] Ricardo Lagos Escobar, citado por: Proyecto de Reforma y Modernización del Estado - Ministerio Secretaría General de la Presidencia y Programa de Modernización de la Gestión Pública - Departamento de Ingeniería Industrial - Universidad de Chile. Gobierno Electrónico en Chile: Estado del Arte. Santiago de Chile, 2003. p. 44.

[57] Proyecto de Reforma y Modernización del Estado - Ministerio Secretaría General de la Presidencia y Programa de Modernización de la Gestión Pública - Departamento de Ingeniería Industrial - Universidad de Chile. Gobierno Electrónico en Chile: Estado del Arte. Santiago de Chile, 2003. p. 10.

[58] Servicio de Impuestos Internos. SII Internet. Hacia un gobierno electrónico [en línea] <http://www.sii.cl/sii_internet/sii_internet.htm> [consulta: 20 de noviembre de 2005].

Finalmente, el Banco Mundial señala que el vocablo Gobierno Electrónico se refiere al uso de Tecnologías de la Información por parte de las agencias gubernamentales. "Estas tecnologías poseen el potencial para transformar las relaciones con la sociedad y pueden perseguir diversos fines, como mejorar la calidad de los servicios gubernamentales a los ciudadanos, promover las interacciones con las empresas e industrias, fortalecer la participación ciudadana a través del acceso a la información y más eficiente administración gubernamental."[59]

De esta forma, una definición que intente abordar los ámbitos y alcances expuestos en las definiciones anteriores es entender el Gobierno Electrónico como el uso de TIC por parte de los órganos de la Administración del Estado para mejorar cualitativamente los servicios e información por ella ofrecida a los ciudadanos, aumentar la eficiencia y eficacia de la gestión pública e incrementar sustantivamente la transparencia del sector público y la participación ciudadana, mediante el diálogo virtual. Es así como los principios de eficiencia y eficacia se han constituido en pilares del Gobierno Electrónico. Por esto es que la definición propuesta se refiere tanto a los aspectos tecnológicos como a la gestión de los órganos de la Administración del Estado, buscando alcanzar mayores niveles de eficiencia y eficacia en el quehacer gubernamental.

Como queda claro, la necesidad de que la Administración del Estado posea aplicaciones eficientes y eficaces en las distintas actividades que desarrolle por medios electrónicos es fundamental para su éxito. Además, teniendo en cuenta que el artículo 20 de la ley N° 19.628, sobre protección de los datos de carácter personal autoriza a los órganos de la Administración del Estado al tratamiento de datos personales con respecto de las materias de su competencia y con sujeción a las reglas determinadas, sin necesidad del consentimiento del titular, la eficiencia y eficacia de la seguridad se torna relevante.

[59] The World Bank Group. A definition of e-government [en línea] <www.worldbank.org/publicsector/egov/definition.htm>. [consulta: 28 de noviembre de 2005]

3.- Principales actividades públicas realizadas por medio del Gobierno Electrónico en Chile.

A estas alturas ya estamos en condiciones de establecer las principales actividades que la Administración del Estado desarrolla mediante las TIC. Como ya adelantáramos, los sujetos que interactúan a través del Gobierno Electrónico son, en un primer lugar, los órganos de la Administración del Estado, quienes se relacionan con los particulares, sean estas personas naturales o jurídicas, asociaciones o agrupaciones, con o sin fines de lucro. Además, los distintos órganos de la Administración del Estado interactúan entre sí y con sus empleados.

La Agenda de Gobierno Electrónico 2002 – 2005 estableció que las posibilidades que se abren con el impulso de la modernización tecnológica de la Administración del Estado, y por lo tanto herramientas en pos del bien común, son:

- "Tener nuevas y variadas alternativas de acceso a las prestaciones de servicios de las instituciones del Estado."

- "Emplear cotidianamente la firma electrónica como medio de identificación, adoptándose modalidades de este recurso según corresponda a las necesidades y particularidades de cada proceso, situación, tipo de transacción y nivel de seguridad requerido."

- "Recibir atención y servicio independientemente del lugar donde se viva y se encuentre ubicado el Servicio que otorga la prestación."

- "Recibir atención y servicio las 24 horas, 7 días de la semana, los 365 días del año; independientemente de los horarios de atención presencial que mantenga cada institución."

- "Tener acceso a información pública o personal en forma simple, clara y transparente."

- “Notificar sólo una vez sobre eventos o situaciones de vida a la institución pública que corresponda, encargándose ésta de entregar esta información al resto de las instituciones del Estado.”

- “Pagar o recibir dinero de las instituciones públicas de modo electrónico, para lo cual deberá ser posible realizar transacciones con un número significativo de instituciones privadas.”

- “Realizar todo tipo de transacciones de manera segura y obtener los servicios que se deseen en forma oportuna y con altos estándares de calidad, pudiendo tener registro posterior de todas las transacciones u operaciones que se lleven a cabo.”

- “Consultar información de los actos públicos del Estado que sea de interés conocer. El Estado transparentará dichos actos dejándolos disponibles electrónicamente.”

- “Ejercer el derecho a participar y expresar una opinión por medios electrónicos. De igual manera, tener la posibilidad de comunicarse con autoridades e instituciones públicas a través de canales habilitados especialmente con ese fin, tales como foros, video chat y otras formas virtuales de relación.”[60]

Así, sintetizando las distintas actividades que pueden desarrollar los órganos de la Administración del Estado mediante las TIC, esto es, actividades relevantes que se desarrollan mediante el Gobierno Electrónico, se puede establecer que estas se refieren principalmente a:

- Comunicación, de la Administración con los particulares y entre la Administración misma.

[60] Proyecto de Reforma y Modernización del Estado - Ministerio Secretaría General de la Presidencia. Agenda Gobierno Electrónico 2002-2005. Santiago de Chile, 2002. pp. 6 y 7.

- Proveer de información a los particulares, recabar información en los ámbitos más disímiles de las actividades privadas o públicas y almacenar dicha información.

- Desarrollo de procesos en el marco de los procedimientos administrativos.

- Transferencias electrónicas de dinero.

3.1.- Comunicación entre la Administración y los particulares y entre la Administración misma.

Las situaciones en que puede darse una comunicación entre los particulares y la administración son innumerables, y se refieren principalmente a la posibilidad de ejercer el derecho de participar y expresar una opinión, y a la posibilidad de comunicarse con autoridades e instituciones públicas a través de canales electrónicos habilitados especialmente con ese fin.

Del mismo modo, las instancias en que puede producirse comunicación entre distintos órganos de la misma administración también son variadas, permitiendo optimizar los recursos disponibles evitando, por ejemplo, que funcionarios públicos deban trasladarse físicamente para poder comunicarse.

En consecuencia, las TIC permiten el desarrollo de una comunicación más eficiente y eficaz.

3.2.- Almacenamiento, administración, recepción y entrega de información.

Respecto de la información, es necesario señalar, de partida, que a diferencia de lo que ocurre con la comunicación, donde ésta se desarrolla en dos niveles, en el ámbito de competencias del Gobierno Electrónico la información se aborda desde tres puntos de vista distintos. El primero se refiere a que la Administración provee de información relevante, tanto a los particulares como a otros órganos de la misma Administración; el segundo dice relación con la Administración del Estado como receptora de información

por parte de los mismos sujetos, y el tercero ve a la Administración como ente almacenador de dicha información.

Ahora bien, el problema de la información que se encuentra almacenada en poder de la Administración ha producido gran cantidad de literatura referente a la tensión que existe respecto de los principios de publicidad y de secreto.

Así, se ha dicho que "de un lado, la Administración debe ser transparente y facilitar la información que se le pide, pero, de otro, la Administración está obligada a mantener el secreto en ciertas materias e, incluso necesita de un cierto secreto para poder actuar eficazmente. Ello significa para sus autoridades y funcionarios, un doble deber: el deber de informar y el deber de callar."[61]

En el mismo sentido, el profesor Fernando Sainz Moreno identifica magistralmente esta situación, señalando que "la configuración del secreto en el derecho público es una cuestión muy compleja, sometida a fuertes tensiones contrapuestas. De una parte, el secreto administrativo tiene muy mala prensa. La opinión pública acusa una y otra vez a la Administración de hermetismo, de falta de transparencia: el poder público utiliza la Administración cerrada en sí misma, que se enfrenta al ciudadano como un enemigo cargado de misterios, de asuntos turbios, ilegales, que se ocultan porque no resisten la luz del día (...) Esta situación debe terminar en un Estado de derecho, libre y democrático. El secreto administrativo, o lo que es igual, el secreto del poder, es incompatible con la libertad y hace imposible una real participación ciudadana en los asuntos públicos. Y, sin embargo, al mismo tiempo que se pide transparencia, se exige a la Administración que guarde riguroso secreto en todo aquello que conoce u cuya difusión externa, o comunicación interna, pueda causar algún perjuicio personal, profesional o económico a los ciudadanos."[62]

[61] Fernando Sainz Moreno, citado por Manuel Lucas Duran. El Acceso a los Datos en Poder de la Administración Tributaria. Pamplona. Ed. Aranzadi, 1997. p. 21
[62] Fernando Sainz Moreno, citado por Manuel Lucas Duran. El Acceso a los Datos en Poder de la Administración Tributaria. Pamplona. Ed. Aranzadi, 1997. p. 21

Toda esta discusión tiene especial importancia, ya que en nuestro país existen diversos órganos públicos que manejan información relevante, como por ejemplo el Servicio de Registro Civil e Identificación, o el Servicio de Impuestos Internos (S. I. I.), que es el receptor de información que un sinnúmero de instituciones públicas y privadas están obligadas a proporcionarle, con la finalidad general de evitar que operaciones gravadas con algunos de los distintos impuestos, especialmente impuestos a la renta, puedan ser omitidas u ocultadas por los contribuyentes para evadir los tributos. Esta recepción, almacenamiento y utilización de dicha información llega al extremo de permitirle al S. I. I. proponer una completa declaración de impuestos a aquellos contribuyentes que decidan efectuar dicho trámite vía Internet, basados en la información que manejan.

En esta materia, el artículo 35 inciso segundo del Código Tributario, cuyo texto se contiene en el Decreto Ley N° 830 de 1974, establece que el S. I. I. no podrá divulgar, en forma alguna, la cuantía o fuente de las rentas, ni las pérdidas, gastos o cualquier dato relativo a ellas que figuren en declaraciones obligatorias, ni permitirán que sus copias, libros o papeles que contengan extractos o datos tomados de ellas sean conocidas por persona alguna ajena al servicio, salvo cuando fueren necesarios para dar cumplimiento a las disposiciones legales vigentes, sean solicitados por los tribunales de justicia para la prosecución de los juicios sobre impuestos o alimentos, o los soliciten los fiscales del Ministerio Público. Pues bien, es precisamente esta la información que los contribuyentes otorgan al S. I. I. al realizar casi cualquiera de los trámites que es posible realizar por medios electrónicos.

Ahora bien, la regla general en materia de información en poder del Estado es la publicidad, tolerándose el secreto o reserva en muy específicos casos, que en general, se refieren a la seguridad nacional y a la protección de datos de carácter personal. Es el artículo 8° de la Constitución Política de la República, en la redacción que le introdujera la reforma constitucional de agosto de 2005, materializada por la ley N° 20.050, el que se hace cargo de este tema, estableciendo en su inciso tercero que “son públicos los actos y resoluciones de los órganos del Estado, así como sus fundamentos y los documentos que se utilicen. Sin embargo, sólo una ley de quórum

calificado podrá establecer la reserva o secreto de aquellos o de éstos, cuando la publicidad afectare el debido cumplimiento de las funciones de dichos órganos, los derechos de las personas, la seguridad de la Nación o el interés nacional."

A nivel legal encontramos el artículo 13 de la Ley Orgánica Constitucional de Bases Generales de la Administración del Estado, la que señala que "la función pública se ejercerá con transparencia, de manera que permita y promueva el conocimiento de los procedimientos, contenidos y fundamentos de las decisiones que se adopten en el ejercicio de ella", agregando en su inciso tercero que "son públicos los actos administrativos de los órganos de la Administración del Estado y los documentos que le sirvan de sustento o complemento directo y esencial"; por su parte, el artículo 16 de la Ley sobre Bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración Pública del Estado se expresa en los mismos términos, agregando que "salvo las excepciones establecidas por la ley o el reglamento, son públicos los actos administrativos de los órganos de la Administración del Estado..."

El mismo artículo 13 de la Ley Orgánica Constitucional de Bases Generales de la Administración del Estado, ahora en su inciso 11 establece que "las únicas causales en cuya virtud se podrá denegar la entrega de los documentos o antecedentes requeridos son la reserva o secreto establecidos en las disposiciones legales o reglamentarias; el que la publicidad impida o entorpezca el debido cumplimiento de las funciones del órgano requerido; la oposición en tiempo y forma por los terceros a quienes se refiere o afecta la información contenida en los documentos requeridos; el que la divulgación o entrega de los documentos o antecedentes requeridos afecte sensiblemente los derechos o intereses de terceras personas, según calificación fundada efectuada por el jefe superior del órgano requerido, y el que la publicidad afecte la seguridad de la Nación o el interés nacional."

Como queda en evidencia de la lectura de ambas normas, la constitucional y la legal, el nuevo artículo 8° de la Carta Fundamental ha ampliado el ámbito del principio de publicidad respecto del existente hasta antes de la reforma constitucional de 2005, extendiéndolo no sólo a los actos de la Administración, sino que también a sus

resoluciones. Asimismo, se ha extendido la publicidad a los fundamentos de los actos o resoluciones y a los procedimientos utilizados en cada caso. Así lo ha entendido el Tribunal Constitucional en su fallo de 9 de agosto de 2007, en que declara inaplicable por inconstitucionalidad el artículo 13 inciso 11 de la Ley Orgánica Constitucional de Bases Generales de la Administración del Estado, en cuanto se faculta al jefe superior del órgano a quien se requiere información que califique, por resolución fundada, acerca de si la divulgación de la información solicitada afecta sensiblemente los derechos o intereses de terceras personas, pues, es una facultad que el constituyente no ha dado. Por el contrario, ha señalado determinantemente las causales por las cuales se puede permitir el secreto o reserva y ha dado al legislador de quórum calificado la precisión del contenido y alcance de las causales constitucionales.

En consecuencia, debemos entender que el nuevo artículo 8° de la Constitución Política de la República ha hecho una ampliación importante en cuanto al ámbito en que la Administración del Estado debe respetar el principio de publicidad, y como consecuencia de aquello, ha derogado tácitamente la facultad del jefe superior del servicio para calificar la divulgación de información requerida, contenida en el artículo 13 inciso 11 de la Ley Orgánica Constitucional de Bases Generales de la Administración del Estado.

Ahora bien, la información que el Estado provee en virtud del principio de publicidad y del cumplimiento efectivo del deber de garantizar el bien común, es un elemento fundamental en un Estado de Derecho que esta información sea suficiente, fidedigna y oportuna, y por lo tanto, la información que la Administración mantenga continuamente a disposición de los particulares o aquella que sea solicitada y sea entregada como consecuencia de una petición formal, debe cumplir con dichas características, lo que implica que no deben ser objeto de intervenciones de cualquier tipo que la modifique, dañe, elimine, o permita el conocimiento de información con carácter de reservada, en los términos ya descritos, causando perjuicios en los derechos tanto a los particulares como a la misma administración.

Teniendo en cuenta que nuestros últimos gobiernos han incentivado la puesta a disposición de los particulares gran cantidad de información por medios electrónicos, es indispensable para el cabal cumplimiento de esta obligación el que dicha información se mantenga en sistemas seguros, garantizando así su disponibilidad, integridad y veracidad.

Respecto de la Administración como ente receptor de información, el tema es similar a lo ya expuesto, ya que es muy relevante que la información que sea entregada por medios electrónicos a la Administración sea fidedigna, debiendo evitarse que se produzcan violaciones a la seguridad de los software que la intercepten y conozcan, en caso de tratarse de aquella información que la administración debe guardar en secreto, o la modifiquen, dañen o eliminen en caso de cualquier clase de información.

3.3.- Desarrollo de procesos en el marco de los procedimientos administrativos.

Una de las más relevantes actividades públicas que actualmente pueden realizarse por medios electrónicos es la tramitación de procesos en el marco de los procedimientos administrativos, regulado por la Ley N° 19.880 que establece bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado, promulgada el 22 de mayo de 2005, en que se reconoce expresamente la posibilidad de desarrollar este tipo de procedimiento por medios electrónicos con el mismo valor que los realizados en soporte papel.

Podemos decir que procedimiento administrativo es "una sucesión de actos - trámite vinculados entre sí, emanados de la Administración y, en su caso, de particulares interesados, que tiene por finalidad producir un acto administrativo terminal"[63] el que se encuentra profusamente reglado. En consecuencia, es evidente que el procedimiento administrativo es, finalmente, una serie de actos consecutivos de

[63] Rodrigo Moya García: *El Procedimiento Administrativo Electrónico en Chile.* En su: El Procedimiento Administrativo Electrónico, los desafíos de su implementación. Materiales para el Magíster en Derecho de la Informática y las Telecomunicaciones. Escuela de Graduados. Facultad de Derecho. Universidad de Chile.

comunicación entre la Administración y los particulares, en el que se intercambia información relevante, que tienen como objetivo obtener una decisión formal por parte de un órgano de la Administración del Estado en alguna materia específica.

Es este último factor, la finalidad de obtener una decisión formal de la Administración, la que otorga a esta actividad de la Administración su sello distintivo. Como consecuencia de ello, la Administración puede recabar información de distintas clases, la que puede almacenar en soportes electrónicos, por lo tanto, damos por reproducidos los razonamientos expuestos en virtud del problema del manejo de información por parte del Estado.

Aunque admitimos que excede al concepto legal de procedimiento administrativo, la actividad que realiza el Servicio de Impuestos Internos (S. I. I.) al permitir las declaraciones de impuesto, emisión de documentos tributarios, etcétera, por vía electrónica, también cabrían clasificarse como una especie de procedimiento administrativo, posibles de realizar por medios electrónicos, no obstante tener una regulación específica. En el mismo sentido, otra actividad de gran importancia es la realizada por Chilecompra, donde la Administración del Estado adquiere todo tipo de bienes y servicios por medio de procedimientos de licitación pública realizados a través de Internet.

3.4.- Transferencias electrónicas de dinero.

Esta actividad tiene la particularidad de permitir la transferencias de bienes de manera automática entre dos sujetos ubicados en distintos lugares, lo que se puede realizar también por otros medios, pero aquí se puede hacer con mucha comodidad, y a cualquier hora.

Sin embargo, para lograr la eficacia de este tipo de transacciones se debe tener especial cuidado con la seguridad del software que se utilice, evitando la intercepción de la información que podría permitir la configuración de delitos contra el patrimonio de las personas que intervienen en ella.

Demás está decir que en las transferencias de dinero el Estado y los particulares pueden ser tanto emisores como receptores, según sea el caso.

4.- Formas de enfrentar la seguridad del software en el Gobierno Electrónico.

Ya habiendo establecido lo que debemos entender por seguridad, y visto que la Administración del Estado realiza sus más importantes funciones públicas mediante sistemas equipados con software, daremos un breve vistazo a la forma en que tanto la Administración del Estado como los particulares han abordado el tema de la seguridad del software en el Gobierno Electrónico.

4.1.- Por los particulares: Críticas a la seguridad del software de Gobierno Electrónico en Chile.

Debido al auge que ha tenido en los últimos años el Gobierno Electrónico en nuestro país, lo que se manifiesta en que casi todos los servicios públicos tienen páginas web, se han comenzado a desarrollar auditorias informáticas por partes de entidades privadas, las que tienen como objetivo encontrar y denunciar la vulnerabilidad de que adolecen.

Así, el portal terra.cl, el día 12 de septiembre de 2005 publicó un reportaje en el que señaló que una investigación de expertos nacionales en auditoria informática había concluido que los sitios web del gobierno eran vulnerables a ataques de hackers, debido a que existían fallas en la configuración y programación de los software de aplicaciones web que estos utilizan, lo que hacía el acceso a estos sitios fuese sencillo para cualquier persona que tenga conocimientos relativamente básicos de programación.

Lo importante de recalcar es que quien logre vulnerar los sistemas de seguridad de este software, no sólo está en posición de acceder a la información allí contenida, sino

que también de modificarla, dañarla o eliminarla, lo que tiene importantes consecuencias tanto para la Administración del Estado como para los particulares.

La auditoria fue realizada por los investigadores de RGSC Rodrigo Gutiérrez y Álvaro Olavarría, quienes sólo utilizaron información que se encontraba disponible en la web para cualquier persona, es decir, los expertos de RGSC no contaron con ningún tipo de información privilegiada y sólo usaron datos que cualquiera podría encontrar en buscadores tan populares como Google.

Así, los investigadores buscaban poner a prueba la seguridad de los software de aplicaciones que se utilizan en los sitios web de los órganos de la Administración del Estado, con el único fin de alertar a las autoridades de las fallas de seguridad encontradas, cuya explotación inescrupulosa podría causar serios perjuicios a derechos de las personas que interactúan con la Administración del Estado vía comunicación mediante computadores, y a la propia Administración. Por lo mismo, los resultados pormenorizados de dicha auditoria no fueron entregados al público, reservándolos sólo para aquellos encargados del área informática de los distintos servicios públicos que la requirieran.

RGSC tuvo la idea de realizar esta investigación luego de que el investigador Rodrigo Gutiérrez publicara una falla de seguridad de NIC Chile, en la que se denunciaba una vulnerabilidad de transferencia de zonas en un servidor web. En otras palabras, uno de los sitios de NIC Chile almacenaba un script cgi que mostraba la información de las zonas en su servidor de nombres secundario "secundario.nic.cl", lo que ponía en riesgo a cualquier sitio bajo el dominio .cl.

Una vez publicada la vulnerabilidad, NIC Chile corrigió el problema en un par de días, sin embargo, luego se descubrió que nic.gob.cl estaba utilizando un sistema de similares características (nic.gob.cl/consulta.html). Así, si en ese sitio un usuario buscara, por ejemplo, "minsal", podría ver fácilmente todas las máquinas y direcciones IP que están bajo el dominio minsal.gob.cl, lo que permitiría que cualquier persona que quisiera acceder, con cualquier intención, a los sitios de la Administración del Estado

se ahorre la mitad del trabajo, pues este sitio entrega toda la información de dónde están las máquinas. Por esto, Rodrigo Gutiérrez señala que "ese sitio debería estar sólo disponible para personal autorizado del Gobierno".[64]

Ahora bien, como resultado de dicha auditoria se encontraron fallas en la seguridad del software que expone la información contenida electrónicamente y los sistemas críticos del mismo al acceso de sujetos extraños a la Administración a su intervención y manipulación inescrupulosa a través de Internet, "de hecho, estas fallas han provocado que muchos hackers extranjeros y nacionales hoy se jacten de haber vulnerado a varias de nuestras instituciones."[65]

El mencionado reportaje señala que una de las instituciones públicas más vulnerables sería el Ministerio de Salud, además son decenas los sitios de Gobierno que cuentan con fallas de diversa índole y cuyas vulnerabilidades no demorarían más de 10 minutos en explotarse. Entre ellas se encontrarían los siguientes:

- Presidencia de la República
- Dirección del Trabajo
- Ministerio de Salud
- Conicyt
- Fonadis
- Sernac

[64] Rodrigo Gutiérrez, citado por Anita Arriagada. Sitios de gobierno están a merced de los hackers [en línea] Portal Terra. cl. 12 de septiembre de 2005 <http://www.terra.cl/tecnologia/index.cfm?Id_cat=1719&pagina=1&id_reg=534884&accion=secretos> [consulta: 12 de septiembre de 2005]

[65] Anita Arriagada. Sitios de gobierno están a merced de los hackers [en línea] Portal Terra. cl. 12 de septiembre de 2005 <http://www.terra.cl/tecnologia/index.cfm?Id_cat=1719&pagina=1&id_reg=534884&accion=secretos> [consulta: 12 de septiembre de 2005]

- Superintendencia de Electricidad y Combustibles
- Sercotec
- Ministerio del Interior
- Secretaria General de Gobierno
- Senado

Un elemento muy importante para el desarrollo de nuestro trabajo son los casos de NIC Chile, ya señalados, y el caso del Servicio Nacional de la Mujer (SERNAM), "que en una primera inspección presentó problemas, pero que en una segunda revisión, ya tenía sus sistemas bien protegidos."[66]

La importancia de estos hechos constatados por la investigación de RGSC radica en dos elementos sustanciales; el primero se refiere a que actualmente es posible obtener el estándar de seguridad suficiente para estimar que un software de aplicaciones web es seguro, que ya analizamos, y el segundo es que dicho estándar puede obtenerse actualmente en el software de las reparticiones públicas si es que ellas lo conocen y se deciden a hacerlo.

A pesar de lo anterior, debe consignarse que las vulnerabilidades investigadas no son las únicas existentes, sino que en la auditoria se buscaron sólo algunas de ellas, con el fin de comprobar que el sistema no es seguro. Para lograr esto "se realizó una práctica que se denomina Proof of Concept (PoC). Esta parte de la base de que las vulnerabilidades normalmente se producen por errores en las aplicaciones y, en el

[66] Anita Arriagada. Sitios de gobierno están a merced de los hackers [en línea] Portal Terra. cl. 12 de septiembre de 2005 <http://www.terra.cl/tecnologia/index.cfm?Id_cat=1719&pagina=1&id_reg=534884&accion=secretos> [consulta: 12 de septiembre de 2005]

caso de las aplicaciones web, un investigador al comprobar que existe un error en la misma puede deducir según el mensaje que arroja si existe o no la vulnerabilidad. "[67]

Según los propios investigadores, la investigación deja en evidencia que "los encargados de los servicios de desarrollo web (que pueden ser internos o externos) no estarían haciendo bien su trabajo. El Gobierno de Chile, en los últimos años ha dado un impulso notable a la digitalización del país. No obstante, este gran desarrollo no ha ido a la par con una política de seguridad acorde a la importancia que de forma exponencial se le ha entregado a los sistemas web.[68]"

4.2.- Por la Administración: El software seguro como tema de Estado.

La Agenda Digital 2004-2006, desarrollada por un equipo de profesionales de los ámbitos público y privado, ha hecho un excelente diagnóstico de la forma en que el Estado debe enfrentar la seguridad en el Gobierno Electrónico, señalando que "el sector público descansa sobre una compleja red de infraestructura de información que, como resultado de la creciente interconectividad, está expuesta a amenazas, en un número y variedad cada vez mayores. La protección efectiva de esta infraestructura esencial en el sector público requiere determinar una estrategia de seguridad de la infraestructura digital de este sector, con el fin de reducir vulnerabilidad, mitigar daños, acelerar tiempos de recuperación en caso de fallas o actividades maliciosas, así como lograr identificar causas y/o fuentes de estas actividades para su análisis y/o investigación."[69]

Sin embargo, según Rodrigo Gutiérrez, investigador de RGSC y miembro del Grupo de Acción Digital, redactor de la Agenda Digital Chile 2004-2006, en países como Inglaterra, Suecia, Alemania y Estados Unidos, las políticas institucionales de

[67] Anita Arriagada. Sitios de gobierno están a merced de los hackers [en línea] Portal Terra. cl. 12 de septiembre de 2005 <http://www.terra.cl/tecnologia/index.cfm?Id_cat=1719&pagina=1&id_reg=534884&accion=secretos> [consulta: 12 de septiembre de 2005]
[68] Anita Arriagada. Sitios de gobierno están a merced de los hackers [en línea] Portal Terra. cl. 12 de septiembre de 2005 <http://www.terra.cl/tecnologia/index.cfm?Id_cat=1719&pagina=1&id_reg=534884&accion=secretos> [consulta: 12 de septiembre de 2005]
[69] Grupo de Acción Digital. Agenda Digital Chile 2004-2006. p.29

seguridad son tan relevantes que quienes las implementan de mala forma o no las respetan del todo pueden incluso perder sus cargos.

Ahora bien, en Chile se ha creado una guía de desarrollo web, que sin embargo no es utilizada por todas las instituciones públicas que poseen páginas web, pero "si ésta fuera utilizada por todas las instituciones del Estado, daría buenos resultados y evitaría la mayoría de los problemas de seguridad existentes hoy en día."[70]

La poca importancia que se le da al tema de la seguridad dentro de los órganos de la Administración del Estado, tiene como corolario que la toma de decisiones en pro de la seguridad se produce luego de que las fallas han quedado en evidencia, y no con un criterio proactivo, que impida su existencia. Las medidas de seguridad adoptadas, que muchas veces incluyen la adquisición de equipos y software muy costosos, tienden a crear una idea de seguridad, la que en realidad no existe, no debido a que dichos elementos no cumplan su función, sino porque las fallas en la seguridad de una aplicación web no se solucionan por esa vía.

Así, el mismo reporte de seguridad de RGSC, señala que "el grado de compromiso en este tipo de intromisiones depende casi exclusivamente de la arquitectura del sistema, es decir, cuánto acceso o privilegios tiene la aplicación web por sobre el sistema informático en su totalidad."[71]

En este mismo sentido, Fernando Fuentes, gerente de marketing y desarrollo de la empresa NeoSecure, en reportaje del portal Terra.cl de 13 de septiembre de 2005,

[70] Anita Arriagada. Sitios de gobierno están a merced de los hackers [en línea] Portal Terra. cl. 12 de septiembre de 2005 <http://www.terra.cl/tecnologia/index.cfm?Id_cat=1719&pagina=1&id_reg=534884&accion=secretos> [consulta: 12 de septiembre de 2005]
[71] Anita Arriagada. Sitios de gobierno están a merced de los hackers [en línea] Portal Terra. cl. 12 de septiembre de 2005 <http://www.terra.cl/tecnologia/index.cfm?Id_cat=1719&pagina=1&id_reg=534884&accion=secretos> [consulta: 12 de septiembre de 2005]

plantea que “el haber encontrado vulnerabilidades en algunos sitios de gobierno, evidencia que existe necesidad de mejoras en los controles de seguridad”.[72]

El profesional señala que las denuncias sobre las vulnerabilidades del software de la Administración del Estado “evidencia que efectivamente existen oportunidades de mejora tanto a nivel de organización como de implementación de controles de seguridad.”[73]

Sin embargo, el experto estima necesario no generalizar ya que existen órganos de la Administración de Estado que son tremendamente celosas y efectivas en el ámbito de su seguridad informática, especialmente cuando se trata de información relevante.

Es efectivamente por esto, la disparidad que existe entre los distintos órganos de la Administración del Estado respecto de la seguridad del software de Gobierno Electrónico que utilizan, que se puede afirmar que este tema no ha sido abordado como un problema del Estado, ya que queda de manifiesto que no existen criterios uniformes, aun cuando los profesionales coinciden en que la promulgación, por parte del Instituto Nacional de Normalización (I. N. N.), de la norma NCh2777, basada en la ISO 17799, que ya analizaremos en cuanto forma parte del ordenamiento jurídico relativo al Gobierno Electrónico, es una muy buena señal en este sentido.

Para tener seguridad en las aplicaciones de Gobierno Electrónico es necesario “definir controles, aplicar esos controles, verificar permanentemente su efectividad y generar acciones correctivas cuando se requiera sobre los controles.”[74] Es así que se estima que para que los mecanismos de seguridad sean eficientes y eficaces deben existir, a lo menos, tres tipos de instancia preocupadas de la seguridad de la

[72] Rodrigo Peralta Cáceres. La seguridad no ha sido abordada como un tema de Estado [en línea] Portal Terra. cl. 13 de septiembre de 2005<http://www.terra.cl/tecnologia/index.cfm?accion=bits&id=537031> [consulta: 13 de septiembre de 2005]
[73] Rodrigo Peralta Cáceres. La seguridad no ha sido abordada como un tema de Estado [en línea] Portal Terra. cl. 13 de septiembre de 2005<http://www.terra.cl/tecnologia/index.cfm?accion=bits&id=537031> [consulta: 13 de septiembre de 2005]
[74] Rodrigo Peralta Cáceres. La seguridad no ha sido abordada como un tema de Estado [en línea] Portal Terra. cl. 13 de septiembre de 2005<http://www.terra.cl/tecnologia/index.cfm?accion=bits&id=537031> [consulta: 13 de septiembre de 2005]

infraestructura Informática gubernamental; la primera debe desarrollar proyectos de seguridad y ponerlos en acción; la segunda debe preocuparse de su operación y funcionamiento, y, la tercera, debe auditar permanentemente la presencia de los controles de seguridad y su efectividad.

Las herramientas que permitirían la mantención del nivel de seguridad esperado son las mediciones, auditorias informáticas, que analizaremos, y otros medios, que deberían tener un desarrollo y aplicaciones permanentes. ”Sin este ciclo, la probabilidad de que los controles fallen es bastante alta. De hecho, el supuesto sobre el cual debemos trabajar es que los sitios web serán tarde o temprano utilizados inadecuadamente.”[75]

Según la Agenda Digital 2004-2006, es el Ministerio del Interior quién deberá hacerse cargo de este tema, buscando “establecer y mantener un sistema nacional de respuesta a incidentes cibernéticos, administrar un programa de reducción de amenazas y vulnerabilidades, desarrollar un programa de capacitación en seguridad, asegurar el ciberespacio en que opera el Gobierno y administrar un sistema de cooperación nacional e internacional en materia de seguridad.”[76]

[75] Rodrigo Peralta Cáceres. La seguridad no ha sido abordada como un tema de Estado [en línea] Portal Terra. cl. 13 de septiembre de 2005<http://www.terra.cl/tecnologia/index.cfm?accion=bits&id=537031> [consulta: 13 de septiembre de 2005]
[76] Grupo de Acción Digital. Agenda Digital Chile 2004-2006. p.31

CAPÍTULO IV.
MARCO REGULATORIO ESPECÍFICO DEL GOBIERNO ELECTRÓNICO.

La normativa específica sobre seguridad del software de Gobierno Electrónico se encuentra contenida en la Ley N° 19.799, sobre documentos electrónicos, firma electrónica y los servicios de certificación de dicha firma, especialmente en su Título V, sobre uso de firmas electrónicas por los órganos del Estado, y en los Decretos Supremos N° 77 de 2004, que aprueba norma técnica sobre eficiencia de las comunicaciones electrónicas entre órganos de la Administración del Estado y entre estos y los ciudadanos; N° 81 de 2004, que aprueba norma técnica para los órganos de la Administración del Estado sobre interoperabilidad de documentos electrónicos; y N° 83 de 2004, que aprueba norma técnica para los órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos, todos del Ministerio Secretaría General de la Presidencia (MINSEGPRES), que analizaremos.

1.- Definiciones.

Para comenzar con el análisis de la normativa específica sobre seguridad del software de Gobierno Electrónico, realizaremos un pequeño glosario de términos relevantes establecidos en los Decretos Supremos sobre la materia.

- Autenticación: Proceso de confirmación de la identidad del usuario que generó un documento electrónico y/o que utiliza un sistema informático (Artículo 5° letra a. del D. S. N° 83 de 2004 del MINSEGPRES).

- Confidencialidad: Aseguramiento de que el documento electrónico sea conocido sólo por quienes están autorizados para ello (Artículo 5° letra b. del D. S. N° 83 de 2004 del MINSEGPRES).

- Criptografía: Es la práctica y estudio del cifrado y descifrado de datos que tiene por objeto lograr que el mensaje sólo pueda ser conocido por ciertos individuos

habilitados de acuerdo a algoritmos específicos (Artículo 5° numeral 2. del D. S. N° 81 de 2004 del MINSEGPRES).

- Disponibilidad: Aseguramiento de que los usuarios autorizados tengan acceso oportuno al documento electrónico y sus métodos de procesamiento (Artículo 5° letra e. del D. S. N° 83 de 2004 del MINSEGPRES).

- Documento Electrónico: Toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior (Artículo 2° letra d. de la ley N° 19.799; Artículo 5° numeral 3. del D. S. N° 81 de 2004 y artículo 5° letra f. del D. S. N° 83 de 2004, ambos del MINSEGPRES).

- Documentos Públicos: Aquellos documentos que no son ni reservados ni secretos y cuyo conocimiento no está circunscrito (Artículo 5° letra g. del D. S. N° 83 de 2004 del MINSEGPRES).

- Documentos Reservados: Aquellos documentos cuyo conocimiento esté circunscrito al ámbito de la respectiva unidad del órgano a que sean remitidos, en virtud de una ley o de una norma administrativa dictada en conformidad a ella, que les confiere tal carácter (Artículo 5° letra h. del D. S. N° 83 de 2004 del MINSEGPRES).

  Como ya dijéramos al referirnos al principio de la publicidad, debemos entender que la definición de documento reservado aquí señalada ha quedado derogada tácitamente por el artículo 8° de la Constitución Política de la República en su texto dado por la reforma constitucional del año 2005, en el sentido que la calidad de reservado de un documento debe ser determinada sólo por una ley de quórum calificado, y no por ley simple ni menos por norma administrativa.

- Documentos Secretos: Los documentos que tienen tal carácter de conformidad al artículo 13 de la Ley Orgánica Constitucional de Bases Generales de la

Administración del Estado y su Reglamento (Artículo 5° letra i. del D. S. N° 83 de 2004 del MINSEGPRES).

Del mismo modo que respecto de la definición de documento reservado, el artículo 8° de la Constitución Política de la República ha derogado tácitamente esta definición, en el sentido que la referencia normativa debe hacerse a la norma constitucional y no ya a la Ley de Bases Generales de la Administración del Estado.

- Expediente Electrónico: Documento electrónico compuesto por una serie ordenada de actos y documentos representados en formato electrónico, dispuestos en estricto orden de ocurrencia, de ingreso o egreso en aquél, y que corresponde a un procedimiento administrativo o asunto determinado (Artículo 5° numeral 5. del D. S. N° 81 de 2004 del MINSEGPRES).

- Firma Electrónica: Cualquier sonido, símbolo o proceso electrónico, que permite al receptor de un documento electrónico identificar al menos formalmente a su autor (Artículo 5° numeral 7. del D. S. N° 81 de 2004 del MINSEGPRES y artículo 2º letra f) de la ley Nº 19.799, sobre firma electrónica).

- Firma Electrónica Avanzada: Aquella certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincule únicamente al mismo y a los datos a los que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría (Artículo 5° numeral 8. del D. S. N° 81 de 2004 del MINSEGPRES y artículo 2º letra g) de la ley Nº 19.799, sobre firma electrónica).

- Identificador Formal de Autenticación: Mecanismo tecnológico que permite que una persona acredite su identidad utilizando técnicas y medios electrónicos (Artículo 5° letra k. del D. S. N° 83 de 2004 del MINSEGPRES).

- Incidentes de Seguridad: Situación adversa que amenaza o pone en riesgo un sistema informático (Artículo 5° letra l. del D. S. N° 83 de 2004 del MINSEGPRES).

- Integridad: Salvaguardia de la exactitud y totalidad de la información y de los métodos de procesamiento del documento electrónico, así como de las modificaciones realizadas por entes debidamente autorizados (Artículo 5° letra n. del D. S. N° 83 de 2004 del MINSEGPRES).

- Política de Seguridad: Conjunto de normas o buenas prácticas, declaradas y aplicadas por una organización, cuyo objetivo es disminuir el nivel de riesgo en la realización de un conjunto de actividades de interés, o bien garantizar la realización periódica y sistemática de este conjunto (Artículo 5° letra p) del D. S. N° 83 de 2004 del MINSEGPRES).

- Repositorio: Estructura electrónica donde se almacenan documentos electrónicos (Artículo 5° letra q) del D. S. N° 83 de 2004 del MINSEGPRES)

- Riesgos: Amenazas de impactar y vulnerar la seguridad del documento electrónico y su posibilidad de ocurrencia (Artículo 5° letra r) del D. S. N° 83 de 2004 del MINSEGPRES).

- Sistema Informático: Conjunto de uno o más computadores, software asociado, periféricos, terminales, usuarios, procesos físicos, medios de transferencia de información y otros, que forman un todo autónomo capaz de realizar procesamiento de información y/o transferencia de información.

- Sobre Electrónico: Contenedor electrónico capaz de incorporar uno o más documentos electrónicos, además de una o más firmas asociadas a dichos documentos, cuando se encontrasen firmados (Artículo 5° Nº 15) del D. S. N° 81 de 2004 del MINSEGPRES).

- Usuario: Cualquier entidad (persona, producto o sistema TI externo) que interactúa con el producto o sistema TI. (Artículo 5° numeral 18. del D. S. N° 81 de 2004 del MINSEGPRES). Entidad o individuo que utiliza un sistema informático (Artículo 5° letra t. del D. S. N° 83 de 2004 del MINSEGPRES).

2.- Título V de la Ley N° 19.799, sobre documentos electrónicos, firma electrónica y los servicios de certificación de dicha firma.

La ley N° 19.799, sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma forma parte de la normativa general que es aplicable al Gobierno Electrónico, sin embargo, en su título V, que se refiere a la utilización de la firma electrónica por los órganos de la Administración del Estado, contiene normas que se refieren directamente a la seguridad del software que se utiliza en algunas de sus actividades.

Así, en su artículo 42 inciso segundo señala que el repositorio o archivo electrónico que los órganos de la Administración del Estado que utilicen firma electrónica deben tener, será responsabilidad del respectivo funcionario que lo tenga a su cargo, sin perjuicio de la celebración de convenios de cooperación entre diferentes órganos de la Administración del Estado sobre el resguardo de dicho archivo, o la contratación de una empresa privada para la prestación de este servicio. Además, en su inciso tercero establece que dicho repositorio deberá garantizar que se respeten las normas sobre publicidad o secreto de los documentos, establecidas en la ley N° 18.575, Orgánica Constitucional sobre bases de la Administración del Estado, ya analizada.

La norma descrita responsabiliza al funcionario público o a la empresa privada que tenga a su cargo el archivo electrónico ante cualquier incidente de seguridad. Al respecto cabe preguntarse a que responsabilidad se refiere.

Por un lado, el Estado como ente sujeto en su actuar al principio de responsabilidad, debe responder siempre y en todos los casos en que dichos incidentes produzcan daño al patrimonio de un particular. Pero respecto de la

posibilidad del Estado de repetir en contra del funcionario público, este último debe haber incurrido en responsabilidad según lo establecido en los artículos 114 y siguientes del Estatuto Administrativo, y a nuestro entender, eso ocurre si éste ha tenido alguna injerencia en el desarrollo, implementación, adquisición o análisis de la seguridad del software que se ha vulnerado. De lo contrario, podría darse la situación según la cual, al vulnerarse el software de un órgano de la Administración del Estado que cumple con el estándar de seguridad exigido por la normativa vigente, que como veremos en algunos casos no es muy exigente, aún así se responsabilizaría al funcionario a cargo del archivo electrónico por los incidentes de seguridad.

En lo que se refiere a la empresa privada como prestador del servicio de resguardo, estimamos, en primer término, que el Estado debe responder por los daños que produzcan los incidentes de seguridad en el software objeto de este servicio, en virtud de lo que hemos venido diciendo, y para perseguir su responsabilidad como tercero, sólo podría hacerse si no se ha cumplido con las exigencias de seguridad que deberían siempre quedar claramente estipuladas en el respectivo contrato. Esto debido a que, como es evidente, a la empresa privada no puede aplicársele el Estatuto Administrativo como a los funcionarios y empleados públicos.

Ahora bien, respecto de la garantía de respeto a la normativa sobre la publicidad o secreto de los documentos que el archivo o repositorio debe tener, debemos decir que dicha garantía está dada en gran parte por la seguridad del software en que se contiene, y por lo tanto, no se podrá contar con repositorio o archivo electrónico si este es vulnerable a ataques o incidentes de seguridad que hagan imposible acceder a información de libre acceso público o que permitan a sujetos no autorizados a acceder a determinada información. Como consecuencia de lo anterior, si el archivo o repositorio no es seguro en los términos descritos, sería ilegal para los órganos de la Administración del Estado utilizar documentos electrónicos, lo que como se podrá observar, traería graves consecuencias.

Como salta a la vista, para el cumplimiento cabal, adecuado y eficaz de la ley N° 19.799, es necesario que, al menos, los archivos electrónicos donde dichos documentos deben almacenarse se sostengan sobre software seguro.

A mayor abundamiento, el artículo 43 de la misma ley establece que el repositorio deberá garantizar la seguridad, integridad y disponibilidad de la información en él contenida, por lo que instaura un sistema de respaldo en copias de seguridad y el almacenamiento de dichas copias, y en su inciso tercero señala los requisitos del repositorio en función de sus características, las que son:

a. Medidas de seguridad y barreras de protección, frente al acceso no autorizado de usuarios.

b. Contar con monitoreo y alarmas que se activen cuando ocurra un evento no autorizado o fuera de programación, para el caso de fallas en la medidas de seguridad del acceso.

c. La sustitución de la información, por la versión más reciente que se disponga, en el menor tiempo posible, en casos de alteración no programada de aquella.

d. La existencia de un programa alternativo de acción que permita la restauración del servicio en el menor tiempo posible, en caso que el repositorio deje de operar por razones no programadas.

De las características que debe tener el repositorio recién señaladas, es sintomático que sólo aquella contenida en la letra a. se refiera a la seguridad como medio de prevención de ataques o alteraciones a la información, mientras que las señaladas en las letras b., c., y d. se refieren a medidas que deben estar disponibles en el caso que las medidas de seguridad ya hayan fallado.

Respecto de la firma electrónica, el artículo 44 establece que para los efectos de garantizar la publicidad, seguridad, integridad y eficacia en el uso de firmas

electrónicas, los certificadores de dichas firmas de los órganos y servicios públicos de la Administración del Estado deberán cumplir con normas técnicas equivalentes a aquellas fijadas para los prestadores de servicios de certificación acreditados para el desarrollo de la actividad.

Finalmente, en su artículo 45 se obliga a los órganos de la Administración del Estado a que los documentos electrónicos suscritos por medio de firma electrónica avanzada a contener un mecanismo que permita verificar la integridad y autenticidad de los mismos al ser impresos.

3.- Decreto Supremo N° 77 de 2004 del Ministerio Secretaría General de la Presidencia.

Con fecha 3 de junio de 2004 se promulgó el Decreto Supremo N° 77 del Ministerio Secretaría General de la Presidencia, que aprueba norma técnica sobre eficiencia de las comunicaciones electrónicas entre órganos de la Administración del Estado y entre estos y los ciudadanos, publicado en el Diario Oficial el 23 de diciembre de 2004.

Esta norma señala como su objetivo permitir que las comunicaciones por medios electrónicos efectuadas entre los órganos de la Administración del Estado y entre éstos con personas naturales y jurídicas operen de manera efectiva y eficiente. Llama la atención el vocabulario utilizado, pues habla de comunicaciones efectivas, aunque deberíamos entender que se refiere a la eficacia de dichas comunicaciones. Además, en su artículo 2° la normativa expresa que las comunicaciones reguladas por ella se someterán a los principios de legalidad, efectividad, eficiencia, publicidad y transparencia.

Un primer punto que debemos destacar es que esta norma, por disposición de su artículo 1° inciso primero, regula de manera general y supletoria las comunicaciones por medios electrónicos entre los órganos de la Administración del Estado y entre éstos y los particulares, en todos aquellos ámbitos no regulados por otras normas legales, reglamentarias o administrativas específicas. En este sentido, deberíamos entender

que, en lo relativo a la seguridad, esta norma debería sentar el estándar mínimo al que el Estado está obligado, sin embargo, y como veremos, no en todos los casos es así, ya que existen normas especiales que permiten la mantención de niveles de seguridad más bajos que los aquí establecidos.

Más profundamente, esta norma explicita los requisitos de toda transmisión y recepción de comunicaciones electrónicas en que intervengan órganos de la Administración del Estado. Estas son:

- Que aseguren su disponibilidad y acceso posterior.

- Que los sistemas utilizados por el emisor y el destinatario sean compatibles de modo que técnicamente, permitan las comunicaciones entre ambos, incluyendo la utilización de códigos y formatos o diseño de registro establecidos por los órganos de la Administración del Estado.

Un tema muy importante en relación a la eficiencia y eficacia del Gobierno Electrónico, aunque no es tema central de este trabajo, es la compatibilidad e interoperabilidad de los sistemas, de modo tal que permitan dicha comunicación. Dada la existencia de una amplia gama de sistemas, muchos incompatibles o que no permiten la interoperabilidad entre sí, ¿Debe el Estado promover el uso de sistemas compatibles?, ¿Podría hacerlo?, o ¿Debe el Estado adaptarse a los sistemas de los ciudadanos? Estimamos que aún no podríamos dar respuestas a estas preguntas, pero teniendo en cuenta la existencia de sistemas genéricos, estimamos que su utilización por parte de los órganos de la Administración del Estado podría solucionar, en parte, esta problemática.

- Que tengan medidas de seguridad tendientes a evitar la interceptación, obtención, alteración y otras formas de acceso no autorizado a las comunicaciones electrónicas, de conformidad con las normas técnicas generadas por el Comité de Normas para el Documento Electrónico sobre seguridad y confidencialidad del documento electrónico, formalizadas mediante el decreto respectivo.

- Que los órganos de la Administración del Estado designen una o más direcciones electrónicas, que sean consideradas aptas para la recepción de dichas comunicaciones. Estas deberán encontrarse debidamente puestas a disposición o consultables por cualquier usuario.

No nos deja de llamar la atención que esta normativa comience abordando la disponibilidad de los sistemas de comunicación electrónica de forma separada a la seguridad, ya que como vimos, la disponibilidad del sistema es un tema que se encuentra inserto en la seguridad del sistema informático.

Ahora bien, en su artículo 6° se establece la obligación de dejar constancia de la transmisión y recepción de las comunicaciones, obligando a los órganos de la Administración del Estado a asegurar dicha constancia conservando los registros por un período de tiempo que no podrá ser inferior a 6 años, y en su artículo 7° inciso segundo se obliga a cerrar diariamente el registro por medio de un mecanismo manual o automatizado, que garantice su no repudio e integridad, bajo la responsabilidad del encargado de dicho repositorio. Lo mismo se le aplica al registro de eventos de acceso a las respuestas de la Administración, establecido en el artículo 9°. En esta materia, nuevamente la normativa responsabiliza al encargado del repositorio por los incidentes de seguridad que se produzcan, remitiéndonos en este análisis al ya efectuado respecto del artículo 42 inciso segundo de la Ley Nº 19.799, Sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de Dicha Firma.

Respecto de la protección de la confidencialidad de la información, cuando corresponda, el artículo 11 señala que se podrá utilizar un mecanismo de autenticación o de control de acceso a las direcciones electrónicas que contengan las respuestas que dé la Administración del Estado.

Del tenor literal de la norma recién descrita, específicamente por la expresión “podrá”, sería posible entender que la implementación de servicios de autenticación o control de acceso sería facultativo para la Administración del Estado, aún en el caso de

tratarse información confidencial, lo que a la luz de lo ya señalado sería insostenible. Sin duda alguna, y a la luz de lo expuesto sobre la obligación de la Administración de respetar los principios de eficiencia y eficacia, ésta debe implementar dichos mecanismos de autenticación o control de acceso cuando trate con información confidencial.

Finalmente, el artículo 13 establece que las transmisiones y recepciones acreditadas de conformidad con lo señalado en el artículo 6°, ya explicado, serán válidas a efectos del cómputo de plazos establecidos en la ley de bases de los procedimientos administrativos. Esto tiene gran relevancia, ya que el artículo 6º no se refiere directamente a la seguridad del software, sino que al aseguramiento y conservación de las constancias de las comunicaciones por un período determinado de tiempo. Esos registros podrían mantenerse, por ejemplo, respaldados en discos extraíbles que se almacenarían físicamente en lugares determinados, cobrando importancia la seguridad física, esto es, contra desastres naturales, incendios, etcétera, y la capacitación del personal a su cargo. Sin embargo, dichas comunicaciones deben permanecer un tiempo en los computadores, y su aseguramiento pasa, necesariamente, por el software.

¿Que ocurriría, por ejemplo, si habiéndose realizado el respaldo de dichos registros se detecta una incongruencia entre éste y la información contenida en los computadores acerca de un procedimiento administrativo? Nos parece que en el caso de información que se encuentre respaldada debería existir una presunción simplemente legal acerca de la autenticidad de la información contenida en el respaldo, ya que la información contenida en los computadores podría ser modificada más fácilmente al encontrarse conectados con otros equipos, desde los cuales podría vulnerarse el software. Esto porque, como dijimos, un software nunca podrá ser completamente invulnerable, lo importante es que se acerque lo más posible a aquello.

4.- Decreto Supremo N° 81 de 2004 del Ministerio Secretaría General de la Presidencia.

También con fecha 3 de junio de 2004 se promulgó el Decreto Supremo N° 81 del Ministerio Secretaría General de la Presidencia, que aprueba norma técnica para los órganos de la Administración del Estado sobre interoperabilidad de documentos electrónicos, publicado en el Diario Oficial de 23 de diciembre de 2004.

Esta normativa, aunque trata principalmente de la interoperabilidad de los documentos electrónicos, también se refiere a la seguridad del software. Así, en su artículo 16 inciso tercero se establece que deberá garantizarse la autenticidad e integridad del expediente electrónico como asimismo, su disponibilidad y el nivel de confidencialidad que corresponda. En el mismo sentido, el artículo 17 establece la confección de una relación actualizada de los documentos y actualizaciones del expediente, a disposición sólo de quienes tengan derecho a verlo.

Por su parte, el artículo 19 establece que el sobre electrónico deberá dar certeza respecto de la autenticidad, integridad y nivel de confidencialidad del contenido.

La pregunta que cabría hacerse es ¿quién es el responsable por la autenticidad e integridad del expediente o sobre electrónico? Teniendo en cuenta la aplicación general y supletoria del Decreto Supremo N° 77 de 2004, del MINSEGPRES, ya analizado, debería decirse que el responsable es el funcionario público que los tenga a su cargo, reiterando aquí todo lo dicho al analizar aquella norma.

Ahora bien, según el artículo 28, el manejo de los documentos electrónicos deberá hacerse teniendo en consideración condiciones mínimas de seguridad y, en todo caso, dando cumplimiento a las normas técnicas especiales que se fijen para la seguridad y confidencialidad de éstos.

Sorprende que se establezca la obligación de considerar sólo condiciones mínimas de seguridad, haciendo un reconocimiento expreso de la existencia de condiciones de

seguridad mejores que las que el Estado estaría obligado a implementar, y que consecuentemente, están diseñadas para evitar más y de mejor forma los incidentes de seguridad que podrían darse. En otras palabras, una interpretación de esta norma podría dar un margen para que algunos daños que se produzcan por fallas de seguridad del software no fuesen susceptibles de responsabilidad, lo que a nuestro entender, sería inaceptable en virtud de los principios constitucionales y legales que la Administración del Estado debe respetar, la normativa vigente y el régimen de responsabilidad del Estado de Chile.

Lo que podría salvar en alguna medida esta situación es la obligación de dar cumplimiento a las normas técnicas especiales que se fijen para la seguridad y confidencialidad de los documentos electrónicos y la aplicación supletoria del Decreto Nº 77 de 2004 del MINSEGPRES.

Por su parte, el artículo 29 obliga a las autoridades superiores de los órganos de la Administración del Estado a definir políticas para asegurar el cumplimiento de un conjunto de buenas prácticas, entre las cuales se encuentra que todo esquema definido será público, la libre disponibilidad y persistencia de los documentos, salvo que su contenido tenga el carácter de confidencial o secreto, situación en la cual a éste se le podrá dar el mismo tratamiento.

Finalmente, debemos decir que esta norma tiene plazos para su implementación, establecidos en su artículo segundo, desarrollándose en tres etapas: la primera, treinta días contados desde la entrada en vigor del decreto, esto sería, el 22 de enero de 2006, la segunda a más tardar el año 2006; y la tercera a más tardar el año 2009.

5.- Decreto Supremo N° 83 de 2004 del Ministerio Secretaría General de la Presidencia.

Al igual que los Decretos Supremos N° 77 y 81, con fecha 3 de junio de 2004 se promulgó el Decreto Supremo N° 83 de la Secretaría General de la Presidencia, que aprueba norma técnica para los órganos de la Administración del Estado sobre

seguridad y confidencialidad de los documentos electrónicos, publicado en el Diario Oficial de 12 de enero de 2005.

Esta norma, el más extenso de los Decretos Supremos estudiados, es también el más importante, pues, trata específicamente de la seguridad del documento electrónico, la que, indudablemente, está dada en gran medida por la seguridad del software que soporte dichos documentos.

Debemos comenzar estableciendo que en su artículo primero declara que ella establece las características mínimas obligatorias de seguridad y confidencialidad que deben cumplir los documentos electrónicos de los órganos de la Administración del Estado, y las demás cuya aplicación se recomienda para los mismos fines.

Así, en esta norma técnica existen, por un lado, exigencias, obligatorias para los órganos de la Administración del Estado, y por otra, meras recomendaciones, que por lo tanto, no son obligatorias para la Administración, y cuya finalidad y objetivo es garantizar estándares mínimos de seguridad en el uso, almacenamiento, acceso y distribución del documento electrónico; y salvaguardar el uso del documento electrónico de manera segura, confiable y en pleno respeto a la normativa vigente sobre confidencialidad de la información intercambiada.

El fundamento de esta normativa es que los documentos electrónicos constituyen un activo para la entidad que los genera y obtiene. La información que contienen es resultado de una acción determinada y sustenta la toma de decisiones por parte de quien la administra y accede a ella, como lo establece su artículo 3°.

Como se observa, la norma entiende la información como un activo y sustento de la toma de decisiones no sólo respecto de la Administración del Estado, sino también respecto de los particulares, por lo que debemos entenderla como una garantía para los particulares, en el sentido de que la información que obtengan por medio de comunicación electrónica con la Administración deberá estar siempre disponible y ser confiable.

Ahora bien, la norma está diseñada para su cumplimiento en dos etapas, de conformidad con dos niveles, a saber:

- Nivel 1: Nivel básico de seguridad para el documento electrónico, que debió ser implementado por los órganos de la Administración del Estado a más tardar en el año 2004, y

- Nivel 2: Nivel avanzado de seguridad para el documento electrónico, que deberá ser implementado a más tardar en el año 2009.

Respecto de la seguridad, en términos generales, y de acuerdo con lo establecido en el artículo 6°, los atributos esenciales, por lo tanto, mínimos que se deben garantizar son 4:

- Confidencialidad;

- Integridad;

- Factibilidad de autenticación, y

- Disponibilidad.

Respecto del primer atributo, esto es, la confidencialidad, bien cabe recordar que según nuestra legislación los documentos en poder de la Administración del Estado son esencialmente públicos, a menos que las características de su contenido se encuentren entre las descritas, principalmente, por el artículo 13 inciso 11 de la Ley Orgánica Constitucional de Bases Generales de la Administración del Estado. Por esto, nos parece que para mantener la concordancia en la normativa sobre el tratamiento de documentos públicos esta norma debería establecer como atributo esencial la publicidad de los documentos electrónicos, señalando que la confidencialidad será atributo sólo de aquellos documentos que deban ser mantenidos en reserva o secreto

en virtud de las disposiciones legales vigentes. Sin embargo, esta situación podría salvarse al señalar como atributo la disponibilidad del documento. De todas formas, nos parece que lo más acertado hubiese sido tratar normativamente la confidencialidad como un atributo especial y excepcional, aunque de gran relevancia en los casos que corresponda.

Estos cuatro atributos constituyen el concepto de seguridad del documento electrónico al que se sujetan los órganos de la Administración del Estado. Además, por disposición de su artículo 8° inciso primero los órganos de la Administración del Estado están obligados a aplicar las disposiciones del Decreto Supremo, que tienen como objetivo garantizarlos.

Por su parte, en el artículo 7°, se señalan las acciones cuya ejecución permanente permiten obtener y sostener los atributos esenciales de los documentos electrónicos, que son:

- Desarrollar y documentar políticas de seguridad de uso, almacenamiento, acceso y distribución del documento electrónico y de los sistemas informáticos utilizados en su procesamiento.

  Indudablemente, cuando esta norma se refiere a los sistemas informáticos utilizados en el procesamiento de los documentos electrónicos, se está refiriendo a sistemas que tienen como herramienta fundamental al software.

- Diseñar y documentar los procesos y procedimientos para poner en práctica las políticas de seguridad;

- Implementar los procesos y procedimientos señalados precedentemente;

- Monitorear el cumplimiento de los procedimientos establecidos y revisarlos de manera de evitar incidentes de seguridad;

- Concienciar, capacitar y educar a los usuarios para operar los sistemas informáticos de acuerdo a las exigencias establecidas, y

- Definir y documentar los roles y responsabilidad de las entidades e individuos involucrados en cada una de las acciones mencionadas.

Ahora bien, el artículo 8° inciso segundo es de vital importancia para entender la relación existente entre la eficiencia y la seguridad en el Gobierno Electrónico, ya que establece que "no obstante, la consecución y mantención de tales atributos por parte de cada órgano de la Administración del Estado estarán sujetas a la consideración de factores de riesgo y factores de costo/beneficio. Estos últimos podrán invocarse mediante una resolución fundada del jefe de servicio correspondiente, basada en un estudio de análisis de riesgo y/o costo beneficio."

La disposición recién citada, y de acuerdo con su tenor literal, nos dice que los atributos mínimos que se deben garantizar con el fin de obtener seguridad en los documentos electrónicos en poder de los órganos de la Administración del Estado son obligatorios sí y sólo sí existen factores de riesgo que lo ameriten, o que un análisis de costo/beneficio así lo establezca. En otras palabras, si un análisis de los costos que implicaría implementar dicha medidas de seguridad son mayores que los beneficios de no hacerlo, o sea, que se estime innecesario o ineficiente, se permitiría a la Administración mantener software inseguro.

Según las explicaciones que hemos estado desarrollando desde el comienzo de este trabajo, la publicidad, la confidencialidad, la factibilidad de autenticación y la disponibilidad de los documentos son atributos sine que non para hablar de seguridad del software de Gobierno Electrónico. Si en virtud de lo establecido en el artículo 8° inciso segundo estos atributos deben obligatoriamente conseguirse excepto si un informe de riesgo lo considera innecesario, debemos necesariamente concluir que para esta norma los órganos de la Administración del Estado podrán mantener los documentos en software inseguro si un estudio determina que el nivel de seguridad es suficiente, incluso pudiendo no cumplir siquiera con los requerimientos mínimos de

seguridad establecidos en la norma, lo que a todas luces es una contradicción con los principios de eficiencia y eficacia.

Otra forma de interpretar dicho artículo es que se podrán mantener los documentos en software inseguro si se determina que el riesgo de producirse un incidente de seguridad es suficientemente bajo como para garantizar sus atributos esenciales de seguridad. Tomando en cuenta las principales acciones públicas desarrolladas por medio de Gobierno Electrónico, deberemos entender que si la comunicación o almacenamiento de información en bases de datos adolece de falta de disponibilidad, de integridad, de capacidad de identificarse fehacientemente o de confidencialidad en los casos pertinentes, podría en algunos casos, no ser relevante.

De adoptarse dicha interpretación, cabría preguntarse ¿cómo se determina, según esta norma, la información que es relevante y la que no?, y la respuesta es a través de un estudio que discrecionalmente podrá invocar el jefe de servicio en una resolución fundada. Ahora bien, ¿que pasa entonces en aquellos casos en que la Administración del Estado maneja datos de carácter personal? Como veremos, este tipo de información tiene protección especial por parte de nuestro ordenamiento jurídico, dada tanto por el artículo 13 de la LOCBGAE, como por la Ley Nº 19.628 Sobre Protección de Datos de Carácter Personal, por lo que respecto de este tipo de información, la Administración del Estado nunca podrá eximirse de mantener software seguro.

Respecto de los factores de costo/beneficio como eximentes de la obligación de mantener documentos electrónicos en software seguro, es evidente que se trata de un argumento de eficiencia, según el cual es posible disponer por medio de un estudio, que el jefe del servicio podrá invocar discrecionalmente mediante resolución fundada, que el establecimiento de software seguro para sostener los documentos electrónicos es, desde la perspectiva de los recursos y necesidades del servicio, ineficiente.

Teniendo en cuenta que en virtud de los principios y normas constitucionales y legales ya analizadas, los órganos de la Administración del Estado deben actuar siempre según criterios de eficiencia en sus ámbitos de competencia, y que la

seguridad en el Gobierno Electrónico es un elemento fundamental para el ejercicio eficiente de las funciones públicas que por este medio se realizan, la norma en comento sólo podría interpretarse en el sentido que se permite a la Administración del Estado ser ineficiente en el Gobierno Electrónico con el fin de ser eficiente presupuestariamente, lo cual resulta, a todas luces, inadecuado.

Este es el dilema más importante al que se enfrentan los órganos de la Administración del Estado en el ámbito de la seguridad informática en general, y en particular del software del Gobierno Electrónico. Por una parte, es evidente que no todos las reparticiones públicas necesitan del mismo nivel de seguridad en el Gobierno Electrónico; piénsese por ejemplo en los medios de comunicación electrónica y la información que maneja el Servicio de Impuestos Internos (S. I. I.), o el Servicio de Registro Civil e Identificación, que deben interactuar en ámbitos muy sensibles con los particulares, que poseen y manejan información de prácticamente todos y cada uno de los habitantes de la República, y que en su mayoría se constituye por datos de carácter personal, especialmente protegidos por nuestra legislación, o, por otra parte, en órganos de la Administración del Estado que realicen procedimientos administrativos electrónicos, o en órganos que no manejan datos personales o no realicen procedimientos administrativos electrónicos.

Otra importante arista de este tema lo constituye el hecho de que casi todos los órganos del Administración del Estado utilizan la información obtenida por medios electrónicos como base de sus decisiones, y muchas veces también los particulares utilizan la información que el Estado, cualquiera sea el órgano específico, pone a su disposición por medios electrónicos para tomar decisiones.

Un visión radicalizada del asunto argumentaría que el artículo 8º inciso segundo del Decreto Supremo Nº 83 de 2004 del MINSEGPRES, debe considerarse inconsistente con el resto de la normativa, y como una demostración más de la poca importancia que se la da al tema de la seguridad del software en el Gobierno Electrónico en nuestro país. Sin embargo, no es posible negarse a la idea de que los distintos órganos de la Administración del Estado requieren, por las características de sus funciones y sus

particularidades, software con niveles de seguridad distintos. Y esta idea debe entenderse enmarcada precisamente dentro de las consecuencias de la aplicación de los principios de eficiencia y eficacia.

Ahora bien, como ya señaláramos, esta norma establece dos niveles de seguridad, uno básico y uno avanzado.

El primer nivel de seguridad o nivel básico, busca en términos generales, garantizar las condiciones mínimas de seguridad y confidencialidad de los documentos electrónicos, facilitar la adopción de requerimientos de seguridad más estrictos por aquellos organismos, en aquellos tópicos que se estimen necesarios, y la facilitar el Nivel Avanzado de seguridad en aquellos organismos cuyo desarrollo institucional lo requiera.

Por disposición del artículo 11, dentro de cada institución pública deberá establecerse una política que fije las directrices generales que orientan la materia de seguridad, la que debe reflejar claramente el compromiso, apoyo e interés en el fomento y desarrollo de una cultura de seguridad institucional, la que debe incluir como mínimo:

- Una definición de seguridad del documento electrónico, sus objetivos globales, alcance e importancia;

- La difusión de sus contenidos al interior de la organización; y

- Una reevaluación periódica, a lo menos, cada tres años.

Como ya esbozáramos, estimamos que si bien la tarea de fijar las directrices de seguridad es una tarea que debería ser abordada por un solo organismo para toda la Administración del Estado, es indudable que las características propias de cada institución podrían justificar esta norma. Sin embargo, respecto de la definición de seguridad del documento electrónico no encontramos ninguna razón que justifique que

su determinación sea hecha por cada órgano y no se explicite una definición general aplicable a todos ellos, lo que unificaría criterios y podría facilitar un tratamiento más eficaz y eficiente de la seguridad del software.

Además, en este Decreto Supremo se establece la obligación de todos los órganos de la Administración del Estado de tener un encargado de seguridad, que será asesor del jefe de servicio en las materia relativas a la seguridad, siendo sus tareas específicas establecidas en el decreto que lo designe, debiendo cumplir, a lo menos, con la función de tener a su cargo el desarrollo inicial de la política de seguridad al interior del servicio, el control de su implementación y deberá velar por su correcta aplicación, también deberá coordinar la respuesta a incidentes computacionales, que deberemos entender como incidentes de seguridad, y finalmente, deberá establecer puntos de enlace con encargados de seguridad de otros organismos públicos y especialistas externos que le permitan estar al tanto de las tendencias, normas y métodos de seguridad competentes.

El párrafo 4° del título IV se refiere a la clasificación y etiquetado de los documentos electrónicos y sistemas informáticos, que tiene como finalidad indicar la necesidad, prioridad y grado de seguridad, señalándose que el sistema informático deberá tener la clasificación correspondiente a la más alta de los documentos electrónicos que procese. Además, establece que todo documento será asignado implícita o explícitamente a un responsable.

Otra materia importante para el tema de la seguridad es la gestión de las comunicaciones electrónicas, que es tratada por los artículos 22 y siguientes de esta norma, en los que se establece la segregación de las funciones para evitar la negligencia o mal uso del sistema, además de la documentación de los procedimientos de operación de los sistemas informáticos y la incorporación de mecanismos periódicos de auditorias de integridad de los registros de datos almacenados en documentos electrónicos.

Además, se establece la obligación de realizar copias de respaldo de la información y aplicaciones críticas para la institución, debiendo garantizarse la disponibilidad de una infraestructura adecuada de respaldo, para asegurar que estos estén disponibles incluso después de un desastre o la falla de un dispositivo. Esta norma trata la seguridad en el Gobierno Electrónico de una forma reparatoria, esto es, que se toman resguardos para el evento que se produzca, siguiendo la redacción de la norma, un desastre de seguridad.

Por su parte, el artículo 26 señala que los organismos sujetos a dicha norma deberán, en la medida de sus posibilidades, instalar antivirus que proteja frente a la posibilidad de obtener software malicioso por la vía de correo electrónico y proveer mecanismos que permitan proteger la confidencialidad e integridad de los documentos electrónicos, entre otros.

Una vez más, nos sorprendemos ante la ligereza con que la normativa aborda el tema de seguridad, al obligar a los órganos de la Administración del Estado a instalar antivirus y proveer mecanismos que protejan la integridad y confidencialidad del documento electrónico, sólo si está en la medida de sus posibilidades. Nuevamente nos encontramos con un argumento de eficiencia, estableciéndose como sacrificable, en pos de la eficiencia, la seguridad presupuestaria del Gobierno Electrónico.

Otra materia profusamente normada es el control de acceso a los sistemas informáticos, dados por el identificador formal de autenticación, y además, se regula la gestión de continuidad, en virtud de la cual el encargado de seguridad deberá formular un plan de contingencia para asegurar la continuidad de operaciones críticas para la institución.

Ahora bien, el Nivel Avanzado de seguridad se basa en la aplicación de la Norma Chilena NCh2777, que es una homologación de la Norma Internacional ISO/IEC 17799: 2000, siendo idénticas.

Sin embargo, la aplicación que el D. S. da a la NCh2777 no es íntegra, sino que con importantes modificaciones. Así, debemos señalar que la NCh2777 se aplica como nivel máximo de seguridad para el documento electrónico en el ámbito del Gobierno Electrónico, pero sólo respecto de su capítulo 3, con las modificaciones que el D. S. señala; el capítulo 4, salvo los puntos 4.1.5 y 4.1.7, que se toman como meras recomendaciones; la sección 5.1, pero sólo en lo referido a bienes relacionados con el documento electrónico, el punto 5.2.1 y el punto 5.2.2[77] con las modificaciones dadas por el D.S.; las secciones 6.1 y 6.3, tomando la sección 6.2 como mera recomendación; las secciones 7.1 y 7.2, ambas con adecuaciones; el capítulo 8; las secciones 9.1 a 9.4, con adecuaciones, considerando las secciones 9.5 a 9.8 como meras recomendaciones; la sección 10.3, con adecuaciones y el capítulo 11 íntegramente. Además, se excluyen los capítulos 1, 2 y 12.

Dada la magnitud de la aplicación que el D. S. Nº 83 de 2004 da a la NCh2777, efectuaremos sólo una descripción de las materias más relevantes que trata, haciendo los comentarios pertinentes.

En primer lugar, el capítulo 3 trata sobre la determinación, publicación, mantenimiento, revisión y reevaluación de una clara política de seguridad, que el D. S. restringe sólo a los repositorios. La NCh2777 señala como contenido mínimo de dicha política la inclusión de una definición de seguridad de la información, sus objetivos, alcance e importancia, una declaración de intención de la dirección del organismo, una explicación breve de la política de seguridad, una definición de responsabilidades, incluyendo un informe de incidentes de seguridad y una referencia a documentación de apoyo a dicha política de seguridad. Por su parte, el D. S. Nº 83 de 2004 agrega a estos puntos la obligación de establecer indicaciones respecto de los sistemas informáticos, en especial sobre la autorización de instalación y modificación de software y configuración de archivos de los sistemas, indicaciones de uso de la red, e

[77] El artículo 37 letra c) inciso segundo del D. S. Nº 83 de 2005 del MINSEGPRES señala 5.1.2, que no existe en la NCh2777, debiendo entender la referencia hecha al punto 5.2.2, dado el contenido de las modificaciones que el D. S. incorpora al punto.

establecimiento de un sistema de respuesta a incidentes de seguridad y un procedimiento de delegación de autoridad para dar respuesta ante emergencias.

Damos por reproducido aquí lo señalado respecto de la necesidad de que los fundamentos mínimos de la política de seguridad sean comunes a toda la Administración del Estado.

Respecto de la revisión y evaluación, la NCh2777 señala que la política deberá tener un responsable a cargo de su mantención. Señala además que deberá existir un cronograma de revisión periódica sobre la eficacia de la política, el número e impacto de los incidentes de seguridad registrados, el costo e impacto de los controles de eficiencia y los efectos de los cambios de tecnología.

El capítulo 4 se refiere a la seguridad organizacional, estableciendo la creación de un comité de gestión que apoye a la dirección del organismo, haciéndose cargo de la aprobación y revisión de la política de seguridad, de la definición de responsabilidades, y de las iniciativas en pos de la seguridad de la información, además del monitoreo de cambios que hagan más vulnerable la información y de los incidentes de seguridad. También se establece que en organizaciones mayores, como evidentemente es la Administración del Estado, deberá existir un comité en que distintos actores de la organización se coordinen en la implementación de controles de seguridad.

También se hace hincapié en la asignación clara y específica de responsabilidades respecto de la seguridad de la información, identificando y definiendo claramente los diversos bienes y los procesos de seguridad asociados a cada sistema individual.

Otro tema importante tratado en el capítulo 4, cuya aplicación es obligatoria según el D. S. es el establecimiento de un proceso de autorización para las instalaciones de procesamiento de información, que busca asegurar que tanto el hardware como el software de aquellas sea compatible con el ya instalado, que sirva para la tarea que se le pretende asignar y que no menoscabe el nivel de seguridad determinado por la política de seguridad.

Se establece además, que se deberán mantener contactos apropiados con todos aquellos órganos relevantes que tengan ingerencia en la reacción rápida ante incidentes de seguridad, tales como los proveedores de los servicios de información y el operador de telecomunicaciones.

Respecto de la seguridad de la información ante la necesidad de dar acceso a un tercero a la información, por cualquier razón, ya sea este acceso físico, esto es, a las oficinas o computadores de la organización, o lógico, por ejemplo, a una base de datos o a los sistemas de información, se establece que deberá celebrarse un detallado y cuidadoso contrato con quien requiera el acceso, resaltando en él la política de seguridad y los máximos controles y procedimientos sobre métodos y acciones a ejecutar necesarias para el adecuado resguardo de la información. Sin embargo, en el ámbito del gobierno electrónico, dada la gran cantidad de entes públicos y privados que interactúan en este entorno, no siempre es posible celebrar contratos con cada uno de ellos, debiendo establecerse las condiciones de acceso mediante la dictación de normas jurídicas precisas o de la aplicación de normas ya existentes.

La NCh2777, del mismo modo que el nivel básico de seguridad permite la externalización de la gestión y control de todos o algunos de los sistemas de información, lo que deberá efectuarse mediante un contrato que consigne la forma en que se cumplirán las normas, la responsabilidad del agente externo, el resguardo de la integridad y confidencialidad de la información, y la forma de asegurarlo, los controles físicos de acceso, el derecho del organismo para auditar al agente externo, etcétera.

Por su parte, el D. S. establece como mera recomendación la búsqueda de asesoría de un especialista en seguridad de la información y la ejecución de revisiones de la seguridad de la información efectuadas por terceros independientes. Es necesario recalcar aquí que estimamos que una gestión de seguridad que cumpla con estándares aceptables de seguridad no puede abstraerse de la revisión de su sistema por parte de auditores independientes, ya sean estos públicos o privados.

El capítulo 5, en aquella parte que el D. S. hace obligatoria, se refiere a la clasificación y control de los bienes, estableciendo que dichos bienes deberán tener asignado un responsable y que deberá practicarse un inventario de ellos, procediendo a su clasificación con el objeto de identificar la necesidad, prioridad y grado de protección que cada uno de ellos requiera. Sin embargo, el D. S. restringe la aplicación de esta parte de la NCh2777 sólo respecto de los bienes relacionados con el Documento Electrónico.

En un hecho inexplicable, el D. S. 83 de 2004 señala que se aplicará el punto 5.1.2, el que no existe en la NCh2777, debiendo entender que dicha referencia se efectúa al punto 5.2.2, que se refiere al etiquetado y manipulación de la información.

Los capítulo 6 y 7 se refieren a seguridad del personal y seguridad física y del ambiente, que exceden la materia de este trabajo, que es la seguridad lógica del software.

El capítulo 8 se refiere a la gestión de las operaciones y comunicaciones, señalando nuevamente la importancia de establecer responsabilidades y procedimientos claros respecto de las operaciones, señalando que todo procedimiento de operación deberá estar documentado y ser mantenido, salvo cambios autorizados expresamente por la dirección de la organización, que deberán ser adecuadamente identificados y evaluados. Respecto del procedimiento de gestión de incidentes se establece que este deberá señalar los procedimientos particulares para cubrir todos los tipos de incidentes de seguridad potenciales, recuperando tanto la información como la operación del sistema, además de actuar en torno a determinar las causas del incidente, reunir pruebas y evidencias y planificar e implementar soluciones.

Este capítulo analiza también la separación de las responsabilidades, con el fin de reducir el riesgo de un mal uso deliberado o accidental del sistema. También se establece la separación de las instalaciones de desarrollo y operaciones del sistema, ya que las actividades de desarrollo y prueba pueden causar serios daños al sistema

en operación, como la pérdida de archivos. Otra materia tratada aquí es el uso de personal externo para gestionar las instalaciones de procesamiento de información.

La aceptación y planificación del sistema, también tratada en este capítulo, busca que la organización establezca los requisitos de operación de los nuevos sistemas, los documente y pruebe antes de su puesta en operación, además de planificar y prever los requisitos futuros de capacidad y disponibilidad del sistema, evitando así una sobrecarga que pueda desencadenar una falla del sistema.

Un tema de singular importancia es la protección contra el software malicioso. La NCh2777 aplicable al Gobierno Electrónico en virtud del D. S. Nº 83 de 2004, señala, en primer lugar, que deberán establecerse mecanismos de control y procedimientos adecuados para la sensibilización, prevención y detección del software malicioso, debiendo considerarse especialmente políticas formales que exijan el cumplimiento con las licencias de software y medidas de protección contra los riesgos de obtener archivos o software desde redes externas; la instalación, actualización y ejecución permanente de antivirus; revisiones regulares del comportamiento del software; verificación de la inexistencia de virus antes de usar archivos de origen incierto, no autorizado, provenientes de redes no confiables o como archivo adjunto de correo electrónico; establecer planes de continuidad, como un sistema de respaldos y la verificación de toda información relevante relacionada con software malicioso.

La sección referida a la administración interna de los sistemas establece que toda organización deberá hacer respaldos de la información, además de realizar, el personal de operaciones, un registro de todas sus actividades, el que deberá ser objeto de revisión regular por parte de entes independientes del procedimiento de operación a revisar. También se establece un registro de fallas, donde consten los incidentes y la acción correctiva tomada.

Este capítulo también se refiere a la seguridad en la gestión de redes, señalando que deberán tomarse todos los resguardos y controles necesarios para salvaguardar la confidencialidad e integridad de los datos que pasan por las redes.

Respecto de la seguridad en la manipulación de dispositivos no abordaremos el tema de la manipulación de dispositivos removibles y de dispositivos en desuso, pues se refieren a seguridad física, que escapa la materia de este trabajo. Sobre la manipulación de información se establece que este tipo de acciones deben estar claramente estipulados y documentados, desarrollando un procedimiento para cada clase de información, de acuerdo a su clasificación vista respecto del capítulo 5.

Otra materia muy relevante y profusamente tratada por la NCh2777 es el intercambio de información y de software. Se establece la celebración de acuerdos entre las partes que realizarán el intercambio, debiendo señalarse como condiciones de seguridad al menos el régimen de responsabilidades en la gestión para controlar y notificar la transmisión, el despacho y la recepción de la información; el procedimiento para notificar el envío, transmisión, despacho y recepción; normas de identificación del courier; responsabilidad y obligaciones en el evento de pérdida de datos; uso correcto del sistema de etiquetado; determinación sobre la propiedad del software y de la información; normas técnicas para grabar y leer el software y la información y cualquier otro control que sea necesario.

Aquí nuevamente nos encontramos con que la NCh2777 se refiere a la celebración de contratos, sin embargo, creemos que es el sólo ministerio de la ley quien da acceso a los ciudadanos a la información que posee el Estado, principalmente debido a que dicha información es pública por mandato expreso de la ley, salvo si cumple con los requisitos taxativamente señalados en la LOCBGAE, ya analizados

Respecto de la seguridad en el comercio electrónico, se establece la inclusión de controles tendientes a evitar que se produzcan actividades fraudulentas, disputas entre las partes o divulgación o modificación de la información, tales como sistemas de autenticación, verificación de información, etcétera.

La comunicación vía correo electrónico también plantea problemas de seguridad, tales como su intercepción y modificación, o vulnerabilidades derivadas de

direcciones incorrectas o de fallas de disponibilidad del servicio. Por esto, la NCh2777 señala la necesidad de instaurar una política de seguridad y uso correcto del correo electrónico. Muy relacionado con lo anterior se establece un sistema de seguridad en los sistemas de oficina electrónica, como los que posee el Servicio de Impuestos Internos o el Servicio de Registro Civil e Identificación. Entre las medidas propuestas se encuentra la exclusión de aquel sistema de toda información sensible que no pueda ser protegida adecuadamente, y la conservación y respaldo de la información mantenida en el.

El capítulo 9 de la NCh2777 trata sobre el control de acceso a la información, señalándose que deberá establecerse una política de acceso de los usuarios, basándose principalmente en que dicho control esté acorde con la política de clasificación y nivel de seguridad requerido por la información. Respecto del control de acceso la NCh2777 señala el uso de la premisa "se debe prohibir a menos que expresamente se permita". Aquí nuevamente nos encontramos con una clara antinomia, pues si bien en el ámbito del Derecho Público es precisamente esta la premisa que debe seguirse respecto de su aplicación e interpretación, no es menos cierto que por expreso mandato de la ley es pública toda la información del Estado que no se encuentre entre aquellas expresamente calificada de confidencial o secreta. En este entendido, el D. S. debió modificar este punto, señalando que respecto de la información contenida en el entorno del gobierno electrónico "se debe permitir a menos que expresamente se prohíba."

En relación con el acceso de los usuarios al sistema de información se dispone que deben establecerse procedimientos específicos para cada etapa del ciclo del acceso, esto es, desde el registro inicial de los usuarios hasta el registro de término de aquellos que ya no requieren o no deben acceder a determinada información. De este modo, el registro inicial del usuario y la eliminación del sujeto como usuario deberían estar sujetas a un procedimiento que establezca el uso de identificadores o ID's individuales para cada usuario, de modo que pueda rastrearse en el evento que deban asignárseles responsabilidades, además de asegurarse de que el nivel de acceso otorgado sea apropiado y consistente con la política de seguridad y que el usuario firme y conozca

las condiciones de acceso. Además, se establece que los privilegios de acceso, estos son, las facilidades para el usuario de pasar por sobre los controles de identificación, deben reducirse al máximo, registrándose cada usuario y su privilegio, el que deberá ser otorgado sólo si es estrictamente necesario. En este mismo sentido, se establece la necesidad de realizar una revisión periódica de los derechos de acceso.

Pero volviendo al tema de la publicidad de la información que posee el Estado, ¿Es posible que todos quienes tienen de manera general derecho a acceder a aquella información, o sea todos los ciudadanos, deban registrarse?. Nos parece que el sistema debería permitir proteger la información, pero no restringir el acceso a ella de ninguna forma, salvo que, como se ha venido repitiendo, sea de aquellas que la LOCBGAE estima como confidencial o secreta.

La NCh2777 también establece un procedimiento de gestión de contraseñas de los usuarios, que tiende principalmente a su confidencialidad y a establecer claras responsabilidades en contra de quien vulnere esta obligación.

También se trata detalladamente el control de acceso a la red, con el objetivo de que los usuarios no comprometan la seguridad de los sistemas. Esto se logra principalmente mediante el aseguramiento de que existan interfaces apropiadas entre la red de la organización y la red de otras organizaciones, el establecimiento de mecanismos de autenticación para usuarios y equipos y una política adecuada de control de acceso a la red.

El D. S. 83 de 2004 señala que lo establecido en las secciones referidas al control de acceso a la operación del sistema, el control de acceso a la aplicación de sistema de información, el monitoreo de uso del sistema y la sección que trata sobre los computadores móviles y el teletrabajo serán tomadas como meras recomendaciones.

Del capítulo 10, sólo tiene aplicación obligatoria la sección 10.3, referida a los controles criptográficos, pero el D. S. hace la salvedad que respecto de la firma electrónica, tendrán prevalencia las normas de la ley 19.799, sobre documentos

electrónicos, firma electrónica y servicios de certificación de dicha firma. En todo caso, se establece la necesidad de desarrollar una política de uso de controles criptográficos, recomendándose la técnica de encriptación para proteger la confidencialidad de la información crítica. Finalmente se detalla un sistema de protección de claves criptográficas por medio de normas, procedimientos y métodos seguros para generar claves, obtener certificados de clave pública, distribuir, almacenar, cambiar, actualizar y revocar, recuperar, archivar y destruir claves, además de registrar y auditar las actividades relacionadas con la gestión de claves.

Finalmente, el capítulo 11 de la NCh2777, sobre gestión de continuidad del negocio, se aplica íntegramente en virtud del D. S., y trata de la forma de contrarrestar interrupciones del sistema y proteger los procesos críticos, refiriéndose, por tanto, a la disponibilidad de la información. Esto se realiza adelantándose a los hechos, previendo con claridad los eventos que podrían causar una falla o desastre, además de revisarlos periódicamente. Todo el plan de contingencia debe ser conocido por los agentes de la organización, debiendo estar debidamente documentados.

6.- Normativa que indirectamente se refiere a la seguridad del software de Gobierno Electrónico.

La legislación nacional ha abordado un sinnúmero de materias que tocan indirectamente el tema de la seguridad del software de Gobierno Electrónico. Decimos indirectamente porque no son normas dictadas para el ejercicio de las funciones públicas, generales o específicas, por medios electrónicos, pero que por su naturaleza tienen importancia y aplicación en esta materia. Así, las más relevantes son la ley que tipifica figuras penales relativas a la informática y la ley sobre protección de datos de carácter personal.

6.1.- Ley que tipifica figuras penales relativas a la informática.

El derecho penal moderno es la forma que existe para resguardar bienes jurídicos que la sociedad toda ha considerado relevantes, tipificando conductas y asociándolas a

una pena determinada. Respecto de ley N° 19.223 que tipifica figuras penales relativas a la informática, publicada en el Diario Oficial de 7 de junio de 1993, el bien jurídico protegido es "la calidad, pureza e idoneidad de la información contenida en Sistemas de Tratamiento de la misma, así como de los productos provenientes de la operación de dichos sistemas"[78]

Parte de la doctrina actual reconoce que uno de los objetivos del Derecho Penal es la prevención de los delitos, por lo tanto, la ley sobre delitos informáticos es una manera de proteger el software y la información contenida en soporte electrónico sin intervenirlo. Como veremos, dada la tipificación de los delitos este efecto también podría producirse respecto del software del Estado.

Así, esta ley es la primera que se refiere directamente a los sistemas de tratamiento de información y a la información contenida en ellos como bien jurídico protegido, estableciendo penas a aquellas personas que ejecuten ciertos actos en relación a ellos, siendo prolífica en la tipificación de conductas consideradas simple delito en sus escuetos cuatro artículos. Los tipos que podemos identificar son:

- Acceder a un sistema de tratamiento de información con ánimo de apoderarse, conocer o usar indebidamente de la información ahí contenida, con una pena de presidio menor en sus grados mínimo a medio, esto es, de sesenta y un día a tres años (Artículo 2°).

- Alterar o dañar maliciosamente los datos contenidos en un sistema de tratamiento de información, con una pena de presidio menor en su grado medio, esto es, de quinientos cuarenta y un días a tres años (Artículo 3°).

- Destruir maliciosamente un sistema, o componentes o partes de un sistema de tratamiento de información, con una pena de presidio menor en su grado medio a

[78] Alejandro Vera Quilodrán. Delito e Informática: La Informática como fuente de delito. Santiago. Ed. Jurídica La Ley. 1996. p. 103.

máximo, esto es, de quinientos cuarenta y un días a cinco años de prisión (Artículo 1° inciso primero).

- Destruir maliciosamente componentes de un sistema de tratamiento de información que afecte la información ahí contenida, con una pena de presidio menor en su grado máximo, esto es, de tres años y un día a cinco años de prisión Artículo 1° inciso segundo).

- Destruir maliciosamente los datos contenidos en un sistema de tratamiento de información, con una pena de presidio menor en su grado medio, esto es, de quinientos cuarenta y un días a tres años (Artículo 3°).

- Destruir maliciosamente parte de un sistema o un sistema de tratamiento de información que afecte la información ahí contenida, con una pena de presidio menor en su grado máximo, esto es, de tres años y un día a cinco años de prisión Artículo 1° inciso segundo).

- Difundir maliciosamente los datos contenidos en un sistema de tratamiento de información, con una pena de presidio menor en su grado medio, esto es, de quinientos cuarenta y un días a tres años (Artículo 4°).

- Difundir, por parte del responsable de un sistema de tratamiento de información, maliciosamente los datos contenidos en un sistema de tratamiento de información, con una pena de presidio menor en su grado máximo, esto es, de tres años y un día a cinco años (Artículo 4°).

- Impedir maliciosamente el funcionamiento de un sistema de tratamiento de información, con una pena de presidio menor en su grado medio a máximo, esto es, de quinientos cuarenta y un días a cinco años de prisión (Artículo 1° inciso primero).

- Impedir maliciosamente el funcionamiento de un sistema de tratamiento de información que afecte la información ahí contenida, con una pena de presidio menor en su grado máximo, esto es, de tres años y un día a cinco años de prisión Artículo 1° inciso segundo).

- Interceptar un sistema de tratamiento de información con ánimo de apoderarse, conocer o usar indebidamente la información ahí contenida, con una pena de presidio menor en sus grados mínimo a medio, esto es, de sesenta y un día a tres años (Artículo 2°).

- Interferir un sistema de tratamiento de información con ánimo de apoderarse, conocer o usar indebidamente la información ahí contenida, con una pena de presidio menor en sus grados mínimo a medio, esto es, de sesenta y un día a tres años (Artículo 2°).

- Inutilizar maliciosamente componentes o parte de un sistema de tratamiento de información, con una pena de presidio menor en su grado medio a máximo, esto es, de quinientos cuarenta y un días a cinco años de prisión (Artículo 1° inciso primero).

- Inutilizar maliciosamente un sistema de tratamiento de información, con una pena de presidio menor en su grado medio a máximo, esto es, de quinientos cuarenta y un días a cinco años de prisión (Artículo 1° inciso primero).

- Inutilizar maliciosamente componentes o parte de un sistema de tratamiento de información y que afecte la información ahí contenida, con una pena de presidio menor en su grado máximo, esto es, de tres años y un día a cinco años de prisión Artículo 1° inciso segundo).

- Inutilizar maliciosamente un sistema de tratamiento de información y que afecte la información ahí contenida, con una pena de presidio menor en su grado máximo, esto es, de tres años y un día a cinco años de prisión Artículo 1° inciso segundo).

- Modificar maliciosamente el funcionamiento de un tratamiento de información, con una pena de presidio menor en su grado medio a máximo, esto es, de quinientos cuarenta y un días a cinco años de prisión (Artículo 1° inciso primero).

- Modificar maliciosamente el funcionamiento de un tratamiento de información que afecte la información ahí contenida, con una pena de presidio menor en su grado máximo, esto es, de tres años y un día a cinco años de prisión Artículo 1° inciso segundo).

- Obstaculizar maliciosamente el funcionamiento de un sistema de tratamiento de información, con una pena de presidio menor en su grado medio a máximo, esto es, de quinientos cuarenta y un días a cinco años de prisión (Artículo 1° inciso primero).

- Obstaculizar maliciosamente el funcionamiento de un sistema de tratamiento de información que afecte la información ahí contenida, con una pena de presidio menor en su grado máximo, esto es, de tres años y un día a cinco años de prisión Artículo 1° inciso segundo).

- Revelar maliciosamente los datos contenidos en un sistema de tratamiento de información, con una pena de presidio menor en su grado medio, esto es, de quinientos cuarenta y un días a tres años (Artículo 4°).

- Revelar, por parte del responsable de un sistema de tratamiento de información, maliciosamente los datos contenidos en un sistema de tratamiento de información, con una pena de presidio menor en su grado máximo, esto es, de tres años y un día a cinco años (Artículo 4°).

Ahora bien, por la antigüedad de esta ley, que fue dictada hace más de una década, no contiene normas especiales atingentes al software y la información que se

maneja en virtud del Gobierno Electrónico, ya que en aquellos años su desarrollo en nuestro país era aún incipiente.

Las preguntas que cabrían hacerse hoy son ¿es suficiente esta ley para resguardar el software y la información de Gobierno Electrónico?, ¿es necesario establecer una pena calificada para los casos en que la víctima de estos delitos sea la Administración del Estado?

La calificación de las penas supone dar una mayor o menor importancia al bien jurídico protegido en razón de las particularidades que podrían darse en relación al autor del delito o la víctima del delito, entre otras.

Dada la importancia que tiene mantener el software funcionando y el resguardo de la información que maneja el Estado, tanto la que se encuentra abierta al conocimiento público, pero mayormente aquella sobre la cual el Estado tiene la obligación de guardar secreto, se hace necesario el aumento de las penas para aquellos que incurran en los hechos delictuales tipificados en la ley N° 19.223, y que afecten el software y la información de Gobierno Electrónico o del Estado en general, creando el delito electrónico calificado.

6.2.- Ley sobre protección de datos de carácter personal.

Otra ley de aplicación general, y que por tanto es aplicable a la seguridad del software de Gobierno Electrónico es la ley N° 19.628 sobre protección de datos de carácter personal, publicada en el Diario Oficial de 28 de agosto de 1999.

Aunque esta ley se refiere directamente a la protección de los datos de carácter personal en poder el de órganos de la administración del Estado, aborda muy tangencialmente la seguridad del software, señalando en su artículo 11 que “el responsable de los registros o bases donde se almacenen datos personales con posterioridad a su recolección deberá cuidar de ellos con la debida diligencia, haciéndose responsable de los daños.” Ese cuidado diligente que el responsable de los

registros o bases de datos debe tener para con ellos pasa, en gran medida, por mantener dichos datos en software seguro, ya que de no ser así, debería entenderse que dicho cuidado o no existe o no ha sido efectuado con la debida diligencia.

Importante es destacar aquí que el funcionario o empleado público es responsable de sus actos en el sentido del artículo 114 del Estatuto Administrativo, esto es, cuando infringe sus obligaciones o deberes funcionarios, por lo tanto, la sola fuga de información de carácter personal que dicho funcionario tenga bajo su resguardo sería causal para la aplicación de medidas disciplinarias, con independencia de la responsabilidad patrimonial del Estado, en el caso que dicha fuga, además, dañara el patrimonio de algún particular.

En el título IV, sobre el tratamiento de datos por los organismos públicos, su artículo 20 establece que el tratamiento de datos personales por parte de un organismo público sólo podrá efectuarse respecto de las materias de su competencia y con sujeción a las reglas establecidas en la ley. Es interesente señalar que de cumplirse con dichos requisitos no se necesitará del consentimiento del titular de dichos datos para su almacenamiento, y teniendo en cuenta que es el Estado el ente que mayor cantidad de información personal posee, cobra mayor importancia la seguridad del soporte electrónico en que dichos datos se encuentren.

Por su parte, el artículo 21 se refiere a los datos relativos a condenas por delitos, infracciones administrativas y faltas disciplinarias, señalando que ellos no podrán comunicarlos una vez prescrita la acción penal o administrativa, o cumplida o prescrita la sanción o la pena, estableciendo una excepción, cual es que dichos datos sean solicitados por los tribunales de justicia u otros organismos públicos dentro del ámbito de su competencia, obligando a dichos órganos a guardar el debido secreto o reserva respecto de ella, y en todo caso, haciéndoles aplicable lo dispuesto en los artículos 5º, que autoriza al responsable de la base de datos personales a establecer un procedimiento automatizado de transmisión de ellos, siempre que se cautelen los derechos de los titulares y la transmisión guarde relación con las tareas y finalidades de los organismos participantes, dejándose constancia del requirente, el propósito del

requerimiento y el tipo de datos que se transfieren; 7°, que se refiere al secreto que deben guardar las personas que trabajan en el tratamiento de datos personales, tanto en órganos públicos como privados; 11, que hace responsable a quien tenga a su cargo las bases de datos si no ha cuidado de ellos con la debida diligencia; y 18, que limita la entrega de datos que se refiera a obligaciones de carácter económico, financiero y bancario.

Llama la atención que el artículo 21 señale que a los órganos que pueden solicitar la información a que este artículo se refiere le será aplicable la norma del artículo 11, ya analizada, pues podría interpretarse que los órganos de la administración del Estado, a los que se refiere el Título IV de la ley, donde se encuentra dicho artículo 21, están exentos de responsabilidad por la falta de diligencia en el cuidado de ellos, y por tanto, de la mantención de software seguro. Sin embargo, creemos que dicha interpretación es errada, en primer lugar, por el tenor literal de la norma, que señala “en todo caso, les será aplicable lo dispuesto en los artículos... 11°”, lo que para nuestro legislador, generalmente, es un llamado de atención a no olvidar la aplicabilidad de esa norma también en dicho caso; y en segundo lugar, porque los datos a los que se refiere el artículo 21 son de tal importancia que merece un énfasis y un refuerzo en la idea de la obligación de mantener dichos datos seguros, bajo la responsabilidad legal.

El artículo 23 se refiere a la responsabilidad por las infracciones a la ley, señalando que la persona natural o jurídica privada o el organismo público responsable del resguardo de los de datos personales deberá indemnizar el daño patrimonial y moral que causare por el tratamiento indebido de ellos, sin perjuicio de proceder a eliminar, modificar o bloquear los datos de acuerdo a lo requerido por el titular o, en su caso, lo ordenado por el tribunal, señalando además que el monto de la indemnización será establecido prudencialmente por el juez, considerando las circunstancias del caso y la gravedad de los hechos.

La importancia de este artículo radica principalmente en que se reconoce a los órganos de la administración del Estado como susceptibles de responsabilidad extracontractual por los daños patrimoniales y morales que el descuido en el resguardo

de datos de carácter personal cause. Teniendo en cuenta que dichos datos se contienen en gran medida en bases de datos electrónicas, en definitiva, se establece responsabilidad del Estado por los daños derivados de mantener datos de carácter personal en software inseguro.

CAPÍTULO V
EFICIENCIA Y EFICACIA ADMINISTRATIVA VERSUS EFICIENCIA Y EFICACIA DEL SOFTWARE.

1.- Gasto público en Gobierno Electrónico.

El desarrollo, implementación y ejecución del Gobierno Electrónico requiere de la provisión de recursos estatales. Es en virtud de esto que en las partidas de presupuesto de cada una de las reparticiones públicas existe un ítem determinado específicamente para los gastos que realiza el Estado en sus distintos requerimientos.

Como se ha venido diciendo insistentemente, toda actividad del Estado debe guiarse siempre por los principios de eficiencia y eficacia. De esta manera, para que pueda decirse que estos principios están siendo respetados, a lo primero que hay que atender es a la satisfacción de las necesidades con los recursos escasos, ya que mientras mejor, o más eficazmente, se realice una actividad, utilizando los menos recursos posibles, esto es, eficientemente, podemos hablar de una Administración que actúa conforme a los principios que la informan en su actuar. Así, por ejemplo, **"**la experiencia de Finlandia – el país más avanzado en e-gobierno – evidencia que la clave no está en el gasto en tecnologías de información, sino en la asignación inteligente de recursos escasos. En este sentido, el desarrollo del Gobierno Electrónico, debe guiarse por dos criterios básicos. Primero, que existan objetivos claramente establecidos y bien alineados con las prioridades nacionales. Y segundo, que haya una percepción pública acerca de que la mayor eficiencia y efectividad de los servicios públicos se debe, entre otros factores, a la introducción de las nuevas tecnologías de información y comunicación."[79]

Es en este sentido que la iniciativa Nº 16 de la Agenda Digital Chile 2004-2006, se ha caracterizado como "aumentar la métrica y la eficiencia del gasto público en tecnologías de información." Esta iniciativa, según el propio documento, se llevará a

[79] Grupo de Acción Digital. Agenda Digital Chile 2004-2006. p.27

cabo a través de dos vías: el desarrollo de una contabilidad presupuestaria y la adopción, por parte del Estado, de todas aquellas medidas que permitan mejorar la eficiencia. Así, se señala que "en primer lugar, se desarrollará una contabilidad presupuestaria que dé cuenta de la magnitud y eficiencia del gasto público en tecnologías digitales e Internet. Esto es necesario porque el sector público dedica importantes recursos a compras de servicios de telecomunicaciones, compras y/o leasing de hardware, compras de licencias en software, contratación de expertos y empresas para el desarrollo e integración de soluciones informáticas, así como importantes inversiones en la formación de recursos humanos en tecnologías digitales." [80]

"En segundo lugar, el Gobierno impulsará todas las medidas necesarias que permitan aumentar la eficiencia en las compras públicas de tecnologías de información, tal como se está impulsando en el caso de contratos marcos para servicios de telecomunicaciones. En este contexto, el Gobierno utilizará la estandarización de normas técnicas, la interoperabilidad y transparencia de las soluciones informáticas. Esto será fundamental para un desarrollo integrado y seguro de la Red Digital 5D. Adicionalmente, se irán incrementando progresivamente las exigencias de certificación de calidad a las empresas proveedoras de servicios digitales, soluciones informáticas y software. El Ministerio del Interior buscará establecer y mantener un sistema nacional de respuesta a incidentes cibernéticos, administrar un programa de reducción de amenazas y vulnerabilidades, desarrollar un programa de capacitación en seguridad, asegurar el ciberespacio en que opera el Gobierno y administrar un sistema de cooperación nacional e internacional en materia de seguridad."[81]

En cumplimiento de esta iniciativa, la Dirección de Presupuestos (DIPRES), evacuó en junio del año 2004 el "Informe de Cuantificación del Gasto en Gobierno Electrónico Año 2003", el que sin embargo, adolece de una serie de problemas, reconocidos por el mismo informe, que hacen que la información ahí contenida no sea de gran calidad ni muy oportuna. Sin embargo, se trata de un primer paso hacia la consecución de los

[80] Grupo de Acción Digital. Agenda Digital Chile 2004-2006. p.31
[81] Grupo de Acción Digital. Agenda Digital Chile 2004-2006. p.31

objetivos propuestos, aunque desde aquel que no se han publicado más informes. Los problemas del Informe de Cuantificación de Gasto en Gobierno Electrónico año 2003 son principalmente: la limitación de la información sólo al año 2003, su cobertura sólo respecto del gobierno central, la falta de información directa con la que fue desarrollado y la imposibilidad de realizar análisis de tendencia. Aún así, este es el primer y, hasta el momento único, informe que revela de alguna manera el gasto en Gobierno Electrónico.

De esta manera, el informe, para facilitar el análisis, desagregó el gasto en gobierno electrónico en 4 componentes:

- Personal Informático,
- Servicios de Computación y Telecomunicaciones,
- Inversión en Informática, y
- Programas de Implementación y Desarrollo Informático.

Para ser un poco más específico, el informe desarrolló una tabla en la que se profundiza sobre que tipo de actividad compone cada grupo, a saber[82]:

Componente de Gasto	Descripción	Clasificación Presupuestaria
Personal Informático	Considera remuneraciones, viáticos y horas extras, de personal de planta, contrata y honorarios.	Subtítulo 21
Servicios de Computación y Telecomunicaciones	Incluye arriendo de equipos informáticos, servicios computacionales, materiales de uso o consumo corriente, mantenimiento y reparaciones, capacitación y perfeccionamiento del personal informático y gasto en telefonía.	Ítem 22.19:Asignaciones 001, 003, 004 y 005. Ítem 22.21 Asignación 22.16.002

[82] Dirección de Presupuesto. Informe de Cuantificación del Gasto en Gobierno Electrónico año 2003, 2005, p. 3

Inversión en Informática	Considera adquisición de equipos computacionales, operaciones de leasing computacionales, adquisición de sistemas computacionales, programas computacionales, proyectos de diseño y desarrollo de sistemas de información, etc.	Ítem 31.56: Asignaciones 001, 002, 003 y 004.-
Programas de Implementación y Desarrollo Informático	Considera la ejecución de programas relacionados al diseño y desarrollo de Sistemas de Información, de equipamiento de hardware y software y de infraestructura informática en general.	Ítem 25.33 Ítem 33.87

De la tabla expuesta, llama la atención que no se hace referencia expresa a la seguridad como un ítem aparte, ni siquiera en la descripción de los distintos componentes del gasto, y además, la adquisición y desarrollo de software quedan distribuidos entre la Inversión Informática y los Programas de Implementación y Desarrollo Informático. Como consecuencia de esto, deberemos enfocar el análisis en estos dos componentes del gasto público en Gobierno Electrónico.

El Informe también realiza una clasificación de los órganos de la Administración del Estado, basada en la clasificación funcional del gasto confeccionado por el Fondo Monetario Internacional, que clasifica a las instituciones públicas según el propósito para el que fueron creadas. La clasificación del informe distingue entre:

- Funciones Generales: Incluye todas aquellas instituciones vinculadas a la provisión de bienes públicos y servicios que requieren en general el uso del poder obligatorio del Estado, no pudiendo ser provisto por el Sector Privado,

- Funciones Fiscalizadoras: Incluye todas aquellas instituciones que tienen por función la fiscalización de transacciones financieras y no financieras, tanto del sector público como privado,

- Funciones Sociales: Incluye todas aquellas instituciones que entregan un bien o servicio a la comunidad, con un claro sentido social, cumpliendo con ello el rol redistributivo del Estado,

- Funciones Inversoras: Incluye todas aquellas instituciones que tienen por finalidad la ejecución de obras de infraestructura de distinta envergadura, ya sea de tipo social como de apoyo al desarrollo económico del país, y

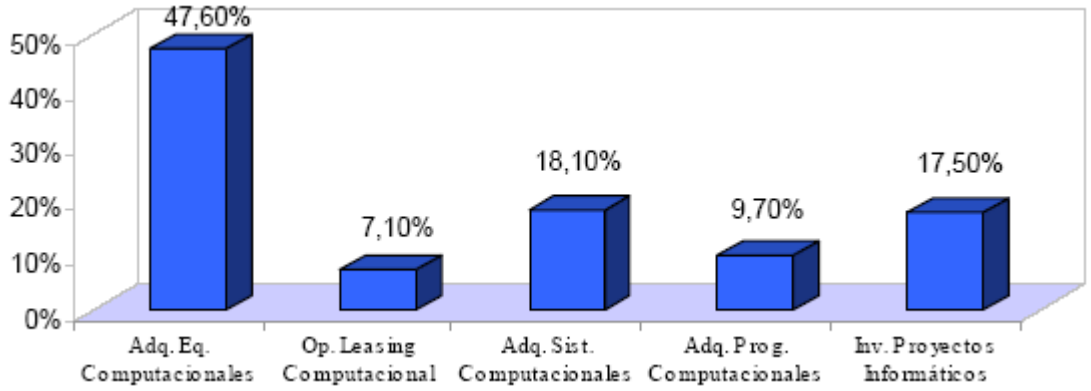
- Funciones Reguladoras: Incluye todas aquellas instituciones que tienen por finalidad principal regular, normar y fomentar actividades públicas y privadas.

Es de la intersección de estos dos elementos, la tipología del gasto en Gobierno Electrónico y la clasificación funcional de los órganos de la Administración del Estado, que el informe desprende sus conclusiones.

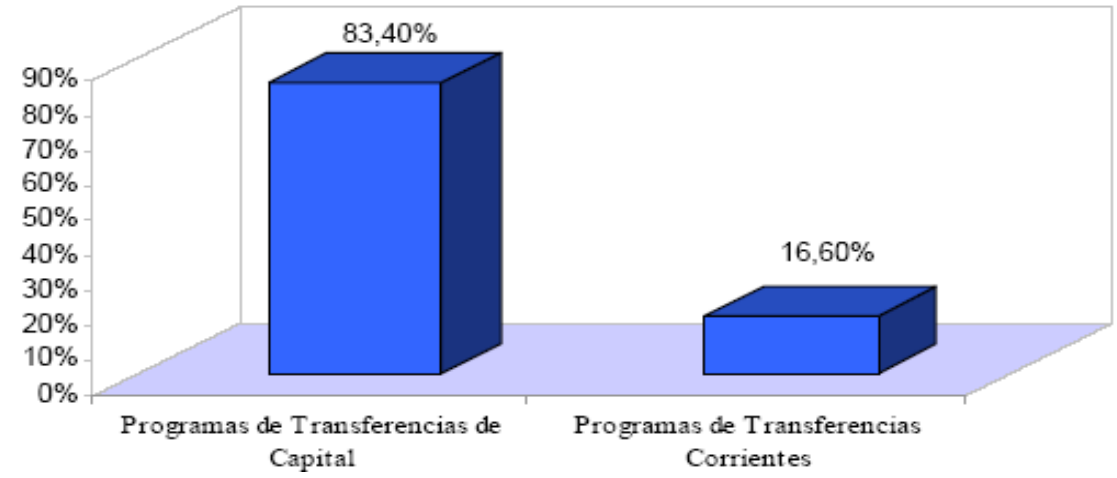
Así, según el informe, en el año 2003 el Estado de Chile gastó $123.088.- millones, de los que $19.835.- millones corresponden a Inversión en Informática, y $14.532.- millones a Programas de Implementación y Desarrollo Informático, siendo estos los ítems de gasto más bajos, correspondiendo a Servicios de Computación y Telecomunicaciones el más alto, con $66.011.- millones, seguido por Personal Informático con 25.710.- millones. Sin duda, estos datos nos indican que, al menos en el año 2003, la atención se encuentra centrada principalmente en los aspectos físicos y en la capacitación de personal.

Confirmando lo anterior, en el área de Inversión Informática, que como vimos representa el 15,7% del gasto en Gobierno Electrónico, se observa que la adquisición de equipos computacionales representa casi la mitad del gasto, mientras que la adquisición de programas computacionales no llega al 10%, como lo expresa el siguiente gráfico[83]:

[83] Dirección de Presupuesto. Informe de Cuantificación del Gasto en Gobierno Electrónico año 2003, 2005, p. 7

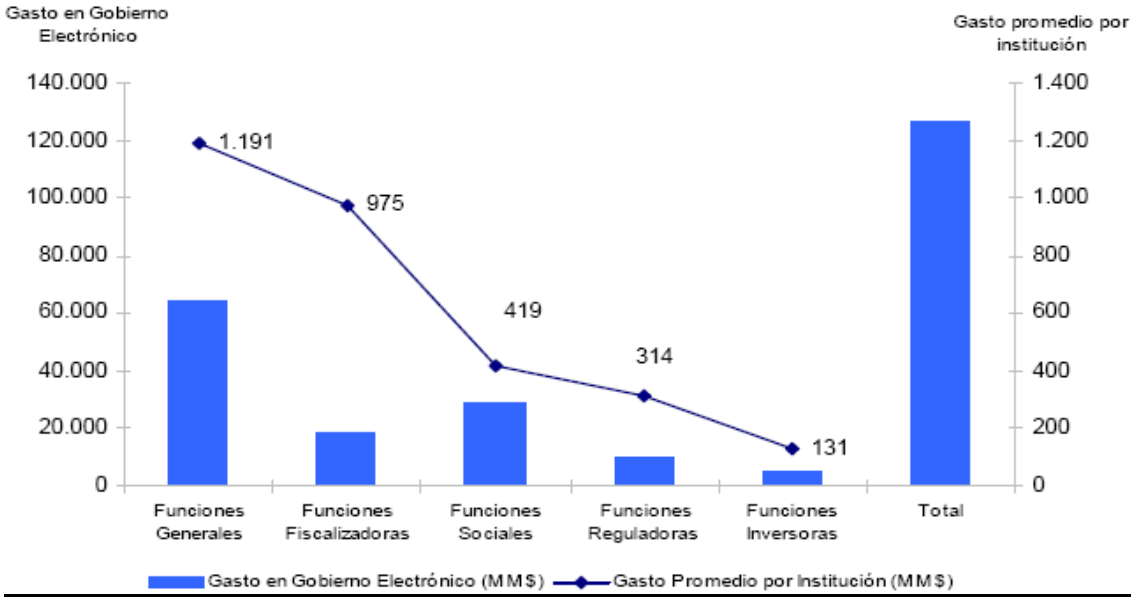


Por su parte, en el área de Programas de Implementación y Desarrollo, que representa el 11,5% del gasto en gobierno electrónico, vemos que el gasto público en programas de transferencia de capital más que quintuplican el gasto en programas de transferencias corrientes. [84]



Ahora bien, para continuar el análisis debemos tener una idea respecto del gasto en Gobierno Electrónico que tienen las instituciones que componen los criterios de clasificación utilizados, y compararlos con el gasto promedio de cada una de aquellas instituciones. La gráfica que nos da el informe da los siguientes resultados[85]:

[84] Dirección de Presupuesto. Informe de Cuantificación del Gasto en Gobierno Electrónico año 2003, 2005, p. 7
[85] Dirección de Presupuesto. Informe de Cuantificación del Gasto en Gobierno Electrónico año 2003, 2005, p. 8

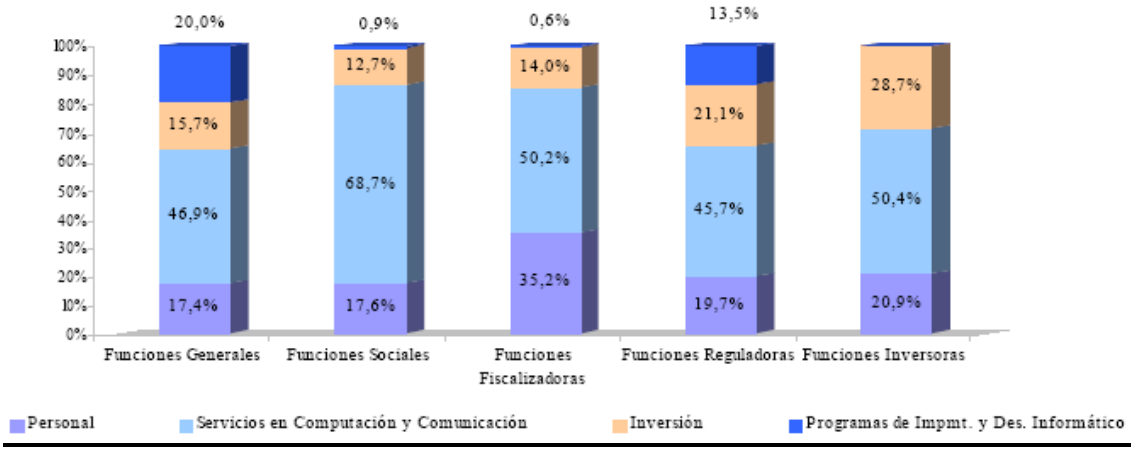


Como se observa, son los órganos de la Administración del Estado que desarrollan funciones generales quienes ostentan el mayor gasto promedio por institución. Teniendo en cuenta que es aquí donde se encuentran la mayoría de los entes públicos que ejecutan funciones de aquellas que hemos denominado monopólicas, llama la atención que sean precisamente ellas quienes más gasto realicen. De la misma forma, también llama poderosamente la atención el promedio de gasto por institución que se observa en las entidades fiscalizadoras.

Sin embargo, los órganos públicos que ejecutan funciones sociales, quienes más directamente interactúan con los particulares en el ejercicio de sus actividades, tienen un gasto promedio bajo en comparación con el gasto total.

Que algunos órganos gasten más que otros no es, hasta ahora, un indicativo de su eficiencia respecto del software, ni menos respecto de su seguridad, por lo que debemos atender a un nuevo criterio, que se refiere al destino que cada una de estas instituciones le da a su gasto en gobierno electrónico.

El informe nos presenta el siguiente gráfico[86]:



Del total del gasto en Gobierno Electrónico, el gasto en Inversión Informática y en Programas de implementación y Desarrollo, no superan el 35%, siendo las funciones generales, reguladores e inversoras quien más destinan a estos ítems, pero con una gran salvedad, las funciones inversoras no tuvieron gasto alguno en Programas de implementación y Desarrollo.

De esta manera, debemos decir que, en primer lugar, no existen datos estadísticos actualizados ni completos como para hacer una medición de eficiencia ni eficacia en el gobierno electrónico, y menos aún para medir la eficiencia y eficacia del gasto en sistemas de seguridad del software, no obstante, y con la poca información con que se cuenta, podemos observar que existe disparidad entre los órganos de la Administración del Estado en cuanto al monto y destino del gasto.

Sin embargo, un reportaje publicado en el portal modernizacion.cl nos ha dado luces acerca de la mayor eficiencia real que el uso de las TIC dan al Estado, al señalar que “la radical reforma al mercado de las compras públicas, impulsada por la reciente entrada en vigencia de la Ley de Compras Públicas, ha sido un importante factor de

[86] Dirección de Presupuesto. Informe de Cuantificación del Gasto en Gobierno Electrónico año 2003, 2005, p. 12

ahorro para la elaboración del Presupuesto del 2004: los gastos fiscales para el próximo año disminuirán en un 5% gracias a la implementación de Chilecompra."[87]

El problema está dado por la obligación y la necesidad para el Estado de mantener software seguro, a través de un plan claro y coherente para que estos niveles de eficiencia y eficacia se logren en todas las reparticiones públicas que operan mediante Gobierno Electrónico, y que dichos niveles no se pierdan.

2.- Eficiencia de las formas de obtener software seguro para el Estado.

El software es, evidentemente, una creación humana, y que éste sea seguro es una característica que como vimos puede o no tener. Por lo tanto, aquí intentaremos analizar algunas formas posibles por medio de las cuales el Estado puede obtener software seguro para cumplir con las tareas a desarrollar mediante Gobierno Electrónico, intentando establecer la conveniencia de optar por uno u otro en virtud de los principios de eficiencia y eficacia.

2.1.- Desarrollo de software seguro por parte del propio Estado.

Una primera forma en que la Administración del Estado podría obtener software seguro es mediante el desarrollo de aquél por parte de ésta. Pero este desarrollo debe ser precisamente lo que se ha denominado desarrollo seguro, el que se puede definir como "el proceso a través del cual se diseña, se implementa y se prueba el software para que sea seguro."[88]

Así, el concepto de desarrollo seguro al que adherimos es muy amplio, ya que se refiere tanto a la seguridad en las aplicaciones, como a la protección de los datos, y de las plataformas que soportan dichas aplicaciones y datos.

---

[87] Proyecto de Reforma y Modernización del Estado. Chilecompra genera importantes ahorros al presupuesto 2004 [en línea] Portal Modernización.cl. 6 de octubre de 2003 < http://www.modernizacion.cl/1350/article-48817.html> [consulta: 23 de marzo de 2006]

[88] Pablo García Pérez. Principios Básicos de Desarrollo Seguro [en línea] <http://www.germinus.com/sala_prensa/articulos/ppos%20basicos%20desarrollo%20seguro.pdf > [consulta: 23 de marzo de 2006]

Como explica el profesor García Pérez, “cuando hablamos de desarrollo seguro nos referimos a la realización o implementación de aplicaciones de todo tipo (lo que quiere decir que no nos referimos solamente a aplicaciones Web, que es en las que se suele pensar más a menudo, sino a todo tipo de aplicaciones) que cumplan una serie de características: que sigan funcionando correctamente frente a cualquier ataque, que den acceso a la información que utilizan sólo a usuarios autorizados (autenticándolos cuando sea necesario), que custodien los datos que manejan y los protejan frente a manipulación consciente o inconsciente de los usuarios y que su disponibilidad esté garantizada.”[89] Como queda en evidencia, el desarrollo seguro tiene, por su naturaleza, como resultado software seguro.

El concepto de desarrollo seguro representa un cambio en el enfoque de la seguridad en el desarrollo del software, ya que la visión tradicional de seguridad se centra simplemente en la protección del software y de los sistemas una vez ya creado el mismo, mediante la utilización de elementos y métodos que buscan reducir las posibilidades de éxito de un ataque sobre él, mientras que “el desarrollo seguro implica pensar en la seguridad del software desde el primer momento y desde las primeras etapas en el ciclo de vida de éste, conociendo y analizando las amenazas que pueden afectar al software que se está desarrollando y definiendo requisitos de seguridad para éste.”[90]

Sin embargo, el mayor problema con que se encontraría la Administración del Estado si intentara obtener software seguro de esta manera sería, en primer término, un problema de constitucionalidad, dado por los límites que la carta fundamental impone a la actividad económica del Estado es sus artículos 1° y 19 N° 21; y en segundo término se encontraría precisamente con un problema de eficiencia, principalmente presupuestaria, en el sentido de que si el Estado asumiera la

[89] Pablo García Pérez. Principios Básicos de Desarrollo Seguro [en línea] <http://www.germinus.com/sala_prensa/articulos/ppos%20basicos%20desarrollo%20seguro.pdf > [consulta: 23 de marzo de 2006]

[90] Pablo García Pérez. Principios Básicos de Desarrollo Seguro [en línea] <http://www.germinus.com/sala_prensa/articulos/ppos%20basicos%20desarrollo%20seguro.pdf > [consulta: 23 de marzo de 2006]

responsabilidad de desarrollar desde cero su propio software acorde a sus necesidades, el costo que esto traería en investigación, innovación tecnológica, apoyo profesional, insumos, etcétera, excedería por mucho el precio que se podría pagar por un software ya desarrollado.

El dilema de seguridad versus costos tiene en esta forma de obtención del software su máxima expresión, pues, el Estado obtendría un software hecho a la medida, con los mayores estándares de seguridad que fuesen necesarios, pero por otro lado, los costos también serían muy altos, requiriendo además de la inversión en desarrollo, la creación y mantención de un equipo técnico propio de la administración para que los beneficios del gran desembolso de dinero en creación puedan persistir, quedando a cargo de este grupo de expertos el servicio técnico que se requiera y la permanente actualización del programa.

Aquí, la pregunta que cabe hacerse es si es o no posible obtener estándares de seguridad similares o mejores a los que se tendrían del desarrollo seguro por parte del Estado utilizando otras formas de más bajo costo. Si la respuesta fuese negativa, sin duda alguna abogaríamos por la utilización de este método como aquel que mejor, o más eficazmente cumple con el mandato constitucional y las normas y principios legales, requiriéndose una ley de quórum calificado para autorizar al Estado a asumir esta actividad económica, según lo dispone el artículo 19 N° 21 de la Constitución, pero si la respuesta es negativa, no queda otra vía que abandonar esta idea. Como veremos e intentaremos explicar, creemos que existen formas más económicas, y por lo tanto eficientes, de obtener software seguro. Además el problema político que se produciría al intentar una ley que dé atribuciones al Estado para abordar por su propia cuenta el desarrollo de software, lo hacen más difícil aun.

2.2.- Adquisición de software.

La forma actualmente más común con la que el Estado obtiene software es la adquisición del mismo a un tercero quien contrata con él, bajo los términos de la Ley N°

19.886 de bases sobre contratos administrativos de suministro y prestación de servicios, publicada en el Diario Oficial el 30 de julio de 2003.

Esta ley, en su artículo primero, define como contrato de suministro aquel que tiene por objeto la compra o el arrendamiento, incluso con opción de compra, de productos o bienes muebles, señalando expresamente como tipos de contrato de suministro, por una parte, "la adquisición y arrendamiento de equipos y sistemas para el tratamiento de la información, sus dispositivos y programas y la cesión del derecho de uso de estos últimos", para señalar luego que "no obstante lo expresado, la adquisición de programas a la medida se considerará contratos de servicios"; y por otra parte, también considera contrato de suministro aquellos que versen sobre el mantenimiento de equipos y sistemas para el tratamiento de la información, sus dispositivos y programas cuando se contrate conjuntamente con la adquisición o arrendamiento.

Como consecuencia del texto legal debemos primero hacer algunas precisiones. En primer término, esta ley no establece expresamente lo que se debe entender como prestación de servicios, debiendo, por lo tanto, analizar las normas de derecho privado para determinarlo. Así, el artículo 2006 del Código Civil señala como contenido del contrato de arrendamiento de servicios "las obras inmateriales, o en que predomina la inteligencia sobre la obra de mano, como una composición literaria o la corrección tipográfica de un impreso…"

Llama la atención que nuestro Código Civil, que data de 1855, señale como contenido del contrato de arrendamiento de servicios la composición de una obra literaria, pues, dichas obras y los programas de computador pueden asimilarse, tal como ocurre respecto del régimen legal y de protección por medio de los derechos de autor. De este modo, podríamos asumir éste como concepto para entender a lo que se refiere la ley de bases sobre contratos administrativos de suministro y prestación de servicios cuando habla de prestación de servicios, ya que establece que la adquisición de programas a medida, o sea, por encargo de la Administración, es una prestación de servicios, al igual que la composición de una obra literaria por encargo.

Así, la adquisición de software puede adoptar dos formas, una primera es la adquisición del programa estándar y su derecho de uso, y la segunda es la adquisición de software encargado a la medida por la Administración. Como vimos, en el primer caso se trata de lo que la ley denomina contrato de suministro, y en el segundo se trata de una prestación de servicios.

Respecto de quien puede contratar con la Administración del Estado en los términos de esta ley, su artículo 4º señala que, en general, "podrán contratar con la Administración las personas naturales o jurídicas, chilenas o extranjeras, que acrediten su situación financiera e idoneidad técnica conforme lo disponga el reglamento…"

Por su parte, los incisos segundo y tercero de dicha norma establecen que "cada entidad licitante podrá establecer, respecto del adjudicatario, en las respectivas bases de licitación, la obligación de otorgar y constituir, al momento de la adjudicación, mandato con poder suficiente o la constitución de sociedad de nacionalidad chilena o agencia de la extranjera, según corresponda, con la cual se celebrará el contrato y cuyo objeto deberá comprender la ejecución de dicho contrato en los términos establecidos en esta ley.

El inciso anterior sólo se aplicará respecto de contratos cuyo objeto sea la adquisición de bienes o la prestación de servicios que el adjudicatario se obligue a entregar o prestar de manera sucesiva en el tiempo."

Esta norma tiene gran relevancia en el ámbito del servicio técnico que deberá acompañar al contrato de suministro o arrendamiento de software, en especial en lo relativo a actualizaciones y corrección de problemas, al que nos referiremos más en detalle al tratar el tipo de software que se está adquiriendo o arrendando.

De esta forma, podemos ya decir que la Administración del Estado puede adquirir dos tipos de software, libre y propietario, situaciones que analizaremos a continuación.

2.2.1.- Software propietario.

La Administración del Estado, por medio del procedimiento que establece la ley de bases sobre contratos administrativos de suministro y prestación de servicios, puede adquirir, en primer lugar, software propietario

Como estableciéramos, el software propietario se caracteriza por una serie de limitaciones, especialmente en su distribución, modificación, copia, etcétera, no pudiendo el usuario acceder a su código fuente. Es el tipo de software que actualmente más se utiliza por la Administración del Estado en nuestro país, aunque algunas administraciones públicas extranjeras, como la española, ya han comenzado a dejarlo de lado.

Una de las características más importantes del software propietario es que para poder utilizarlo de manera que no se vulneren derechos de terceros, su adquisición debe venir acompañada del derecho de uso sobre el mismo, que es precisamente la hipótesis que explicita el artículo segundo de la ley de bases sobre contratos administrativos de suministro y prestación de servicios. En virtud de esto, hay quienes podrían sostener que el Estado sólo puede adquirir software propietario, sin embargo, aquella hipótesis es errónea ya que el listado de operaciones que la ley considera contrato de suministro no es taxativa. Además, el mismo artículo primero de dicha ley señala que el procedimiento que ella establece será aplicable a toda adquisición de bienes muebles que el Estado requiera para el ejercicio de sus funciones, siendo el software libre precisamente aquello.

Las ventajas que daría la utilización de software propietario son, en primer lugar, que se adquiere un programa listo para su uso, evitándose el Estado incurrir en los costos de investigación y desarrollo, que son asumidos por el fabricante, quien al producir software para su venta generalmente masiva, descarga dichos costos en los usuarios que lo adquieren, por lo que se atomizan. Precisamente debido a esto es que también es una ventaja el apoyo técnico especializado que presta el fabricante del software, el que no obstante tener muchas veces un costo adicional, es prestado por

las mismas personas que lo crearon o por agentes autorizados por ellos, y por lo tanto son quienes mejor pueden conocer sus fallas.

Sin embargo, derivado de sus ventajas también encontramos desventajas, principalmente por el hecho que se produce una excesiva dependencia con el proveedor inicial, ya que las actualizaciones suelen ser obligatorias y sujetas a su entera voluntad, y en algunos casos, con un costo no menor. Ahora, si se planteara como solución el cambio a proveedores alternativos, ya sea por descontento o porque las necesidades de la Administración han cambiado, como ocurriría por ejemplo, si se aumentaran los estándares de seguridad, tendría costos muy altos, y supondría, en muchos casos, comenzar de cero en lo que a software se refiere.

Además, "si se utiliza software propietario, sólo su autor original tiene la facultad de corregir errores, agregar funcionalidad, o quitarla, (...) esto hace que el Estado queda sin curso aceptable de acción en muchas situaciones."[91] Como ejemplo podemos señalar:

- La ausencia o demora en la corrección de problemas: "Las prioridades del proveedor de software no son necesariamente las mismas de sus clientes. Si determinado problema de seguridad de un programa no está en la lista de prioridades del proveedor, o si éste se rehúsa a corregirlo o exige una compensación desmesurada para hacerlo (por ejemplo, exigiendo el pago de un upgrade), el Estado no tiene siquiera el recurso de utilizar sus propios medios para obtener una corrección por parte de un tercero."[92]

- Incompatibilidad con versiones previas: "Son conocidos los casos de versiones 'mejoradas' de programas que tienen problemas leyendo datos de versiones anteriores. El cortísimo ciclo de obsolescencia del software, motivado mucho más por razones de marketing que por efectiva demanda de nuevas funcionalidades,

[91] Melisa Tuya. Software abierto software seguro [en línea] <http://www.baquia.es/com//20010418/art00024.html> [consulta: 27 de septiembre de 2005]
[92] Melisa Tuya. Software abierto software seguro [en línea] <http://www.baquia.es/com//20010418/art00024.html> [consulta: 27 de septiembre de 2005]

obliga a los usuarios a mantener su software actualizado, y el precio de la actualización incluye (a menudo sin en conocimiento de los usuarios) la renuncia a acceder a datos valiosos almacenados en archivos."[93]

- Desaparición del proveedor o del producto: "Abundan los ejemplos de programas propietarios cuyos usuarios se vieron obligados a emprender costosísimas migraciones debido a la quiebra del proveedor, a su adquisición por otro más grande, o a la simple discontinuidad del producto por decisión unilateral del autor." [94] Aquí es donde cobran importancia los incisos segundo y tercero del artículo 4° de la ley de de bases sobre contratos administrativos de suministro y prestación de servicios, ya trascritos, pues ninguna de las facultades que dicha norma establece obsta a que ocurra alguna de las hipótesis aquí señaladas.

- Incongruencia entre el software y la ley: "El Estado usa el software para implementar el mandato de la ley. El problema es que cuando existe un conflicto (fruto, quizás, de una diferencia de interpretación) entre el texto de la ley y la función del programa, el ciudadano se encuentra con que el software es más poderoso que la ley, ya que es aquél el que gestiona su trámite, y la solución del problema depende de que el proveedor del programa esté dispuesto a corregirlo, y a hacerlo en un tiempo, forma y presupuesto razonables."[95]

Creemos que el análisis de la profesora Tuya, recién trascrito, describe exactamente uno de los problemas que planteamos desde el comienzo de nuestro estudio, que es el posible enfrentamiento entre el mandato constitucional, legal o reglamentario y los derechos de los titulares del software, en este caso propietario, señalándonos que es el titular del software el único que podría hacer esta adaptación, lo que implicaría subsumir la voluntad legal, y por ende de toda la ciudadanía, a la

[93] Melisa Tuya. Software abierto software seguro [en línea] <http://www.baquia.es/com//20010418/art00024.html> [consulta: 27 de septiembre de 2005]
[94] Melisa Tuya. Software abierto software seguro [en línea] <http://www.baquia.es/com//20010418/art00024.html> [consulta: 27 de septiembre de 2005]
[95] Melisa Tuya. Software abierto software seguro [en línea] <http://www.baquia.es/com//20010418/art00024.html> [consulta: 27 de septiembre de 2005]

voluntad del proveedor, pues de otro modo, deberá el Estado asumir altísimos costos para cambiar al proveedor.

En los contratos de licencia de software propietario siempre se establece una cláusula, que señalaremos a modo meramente ejemplar, es del siguiente tenor: “Protección de la Propiedad Intelectual. El Software, incluyendo su operación, códigos, arquitectura e implementación, junto con la apariencia y sentido de éste, son la preciada propiedad intelectual de (Empresa proveedora). El Software está protegido por las leyes de (País del proveedor, generalmente Estados Unidos) y Chile sobre derechos de autor y las disposiciones de los tratados internacionales. Este Acuerdo no le otorga ningún derecho de propiedad intelectual sobre el Software. Usted está de acuerdo en no modificar, interpretar, desarmar, descompilar, invertir la ingeniería, producir subproductos o hacer ningún intento de ningún modo para descubrir u obtener el código fuente del Software.”

En pocas palabras una lista de ventajas que tendría la Administración del Estado al adquirir software propietario debe contener:

- Que las aplicaciones viene listas para su uso, evitando el Estado asumir todos los costos de investigación y desarrollo.

- Que se cuenta con el apoyo de los fabricantes.

Pero, por otra parte, existe una serie de desventajas, a saber.

- Dificultad para adaptar el software a necesidades específicas;

- Restricciones de distribución;

- Posible ausencia o demora en la corrección de problemas;

- Posible desaparición del proveedor o del producto;

- Posibles Incongruencia entre los derechos del proveedor del software y los derechos de las personas.

2.2.2.- Software libre.

Otro tipo de software que puede adquirir la Administración del Estado es el denominado software libre.

La expresión Software Libre se refiere a la libertad de los usuarios para ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el software. “De modo más preciso, se refiere a cuatro libertades de los usuarios del software:

- La libertad de usar el programa, con cualquier propósito.

- La libertad de estudiar cómo funciona el programa, y adaptarlo a las necesidades del usuario. El acceso al código fuente es una condición necesaria para esto.

- La libertad de distribuir copias.

- La libertad de mejorar el programa y hacer públicas las mejoras a los demás, de modo que toda la comunidad se beneficie. El acceso al código fuente es un requisito previo para esto.”[96]

En estricto rigor lo que ocurre con el software libre no es muy diferente a lo que ocurre con el software propietario, ya que también se distribuye bajo licencia. Lo que los diferencia es precisamente los términos de las licencias en uno y otro caso, ya que tratándose de software libre, no se restringen el uso, la redistribución y la modificación del mismo. Lo que se puede imponer son condiciones a satisfacer precisamente en caso de que se quiera redistribuir el programa. Por ejemplo, se podría exigir que se

[96] The GNU Project. La definición de Software Libre [en línea] <http://www.gnu.org/philosophy/free-sw.es.html> [consulta: 28 de marzo de 2006]

respeten las indicaciones de autoría, o que se incluya el código fuente si se quiere redistribuir el programa listo para ejecutar.

Ahora bien, el uso de software libre significaría, desde ya, un ahorro muy importante para la administración del Estado, sin embargo, además de esto, existen también otros elementos que repercuten directamente en la eficiencia, tanto presupuestaria como en la ejecución de las funciones públicas.

Uno de los elementos más importantes es que, "el software libre no precisa un hardware tan caro como el propietario, por lo que también se reduce el gasto en máquinas."[97]

Siendo tan provechosa la utilización de software libre, cabría preguntarse, por qué no lo adopta la administración del Estado, que tiene como principio básico de su actuar la eficiencia presupuestaria y la eficacia en sus aplicaciones. El especialista José Manuel Gómez, director de la revista online Kriptópolis, responde a esta pregunta señalando que este cambio no se produce "por costumbre. Supone un cambio de mentalidad que requiere que transcurra algo de tiempo."[98] Además reconoce que llevar a cabo la transformación a software libre en sistemas que ya funcionan con software propietario tiene un costo económico inmediato, "es como cambiar toda la red de carreteras, al principio supone grandes costes, que se compensan a mediano plazo. Pero, en cualquier caso, los motivos económicos para nosotros son una consecuencia; lo importante es la seguridad".[99]

Si suponemos que el costo económico de adoptar software libre fuese similar al costo que tendría continuar con el software propietario, debido a los costos de mantenimiento, soporte y personalización que este tipo de software requiere, el cambio acarrearía otros beneficios, especialmente en el desarrollo tecnológico del país, ya que

[97] Melisa Tuya. Software abierto software seguro [en línea] <http://www.baquia.es/com//20010418/art00024.html> [consulta: 27 de septiembre de 2005]
[98] José Manuel Gómez, citado por Melisa Tuya. Software abierto software seguro [en línea] <http://www.baquia.es/com//20010418/art00024.html> [consulta: 27 de septiembre de 2005]
[99] José Manuel Gómez, citado por Melisa Tuya. Software abierto software seguro [en línea] <http://www.baquia.es/com//20010418/art00024.html> [consulta: 27 de septiembre de 2005]

esos costos “revertirían en pequeñas y medianas empresas nacionales para impulsar el sector de tecnologías de la información dentro del país. Que este sector se revitalice dentro del país tal vez les importe poco a las empresas privadas, pero no parece lógico que tampoco les importe a las Administraciones Públicas.” [100]

Ahora bien, si la Administración tiene acceso al código fuente del software que utiliza, puede saber exactamente qué hace el programa, comprobar sus errores o sus agujeros de seguridad y repararlos de la manera que deseen y tan pronto como puedan. “De hecho, con el software abierto es imposible que existan puertas traseras colocadas malintencionadamente por los diseñadores del software por el motivo que sea.”[101]

Existe en círculos académicos el debate acerca de si el software libre es inherentemente más seguro que el propietario, pero no es de esperar que esta cuestión se dirima a corto plazo. “Sí existe consenso, sin embargo, sobre el hecho de que es muchísimo más sencillo esconder código malicioso (puertas traseras, bombas de tiempo, etc.) en software cuyo código fuente no está disponible públicamente que en software que puede ser inspeccionado por cualquier persona interesada y existe numerosa evidencia de funcionalidad escondida en incontables programas propietarios, aún en aquellos producidos por las empresas más prestigiosas.”[102]

Además, “si se carece de la posibilidad de analizar el código fuente, también es imposible determinar si el autor del sistema incluyó mecanismos de inhabilitación temporales o remotos que puedan comprometer la posibilidad de acceso a los datos en el futuro. Asimismo, al usar software propietario, el usuario almacena sus datos mediante el uso de software desconocido, en un formato desconocido. Sin la posibilidad de inspección, es imposible saber si el formato utiliza tecnologías sujetas a

---

[100] Melisa Tuya. Software abierto software seguro [en línea] <http://www.baquia.es/com//20010418/art00024.html> [consulta: 27 de septiembre de 2005]

[101] Melisa Tuya. Software abierto software seguro [en línea] <http://www.baquia.es/com//20010418/art00024.html> [consulta: 27 de septiembre de 2005]

[102] Software Libre Chile. Software Libre en Chile. Misión del Estado [en línea] http://www.softwarelibre.cl/drupal//?q =node/120 [consulta: 23 de marzo de 2006]

patente o derechos de autor, que pudieran resultar en que el acceso a esa información en el futuro dependa de la posesión de las licencias correspondientes."[103]

Otra característica ventajosa de la adopción de software libre es que se evitan, en gran medida, los problemas de ausencia o demora en la corrección de problemas, incompatibilidad con versiones previas, incongruencia entre el software y la ley, y desaparición del proveedor o del producto, que analizamos respecto del software propietario.

Debido a la ventaja de seguridad que tendría el software libre, sería una excelente forma para "asegurar que los datos personales de los ciudadanos en manos de la Administración, así como los secretos oficiales, se encuentren adecuadamente protegidos".[104] Por esto, sería bueno que los encargados de la seguridad del software de Gobierno Electrónico puedan ver el código fuente de, al menos, los sistemas que manejen datos sensibles.

Además, "al emplear software licenciado bajo el modelo propietario, el usuario renuncia a la facultad de tomar ciertas decisiones, ya que éstas le son dictadas por el autor del programa. Estas decisiones van desde la plataforma de hardware (ya que el autor decide sobre qué plataformas ofrecerlo) hasta los programas a usar para tareas relacionadas (ya que el autor se asegura de que sus productos funcionen mejor, cuando no únicamente, al interactuar con otros de su misma factura). Esto lleva a dificultades para garantizar la perennidad de los datos, ya que la obligación de acompañar al proveedor en sus decisiones puede llevar a situaciones insostenibles (por ejemplo, a través de una carrera desenfrenada de actualizaciones de hardware). De la misma manera, la elección de determinado software propietario por parte del Estado limita la libertad de elección del ciudadano en materia de los productos que

[103] Software Libre Chile. Software Libre en Chile. Misión del Estado [en línea] http://www.softwarelibre.cl/drupal//?q =node/120 [consulta: 23 de marzo de 2006]

[104] Melisa Tuya. Software abierto software seguro [en línea] <http://www.baquia.es/com// 20010418/art00024.html> [consulta: 27 de septiembre de 2005]

puede usar para interactuar electrónicamente con la administración pública, lo que constituye una violación de la igualdad de los ciudadanos ante la ley."[105]

Una visión radicalizada considera que "cuando el Estado utiliza software como soporte operativo de sus procedimientos, el mismo pasa a ser parte indisoluble de dichos procedimientos, y por lo tanto está sometido al requerimiento de publicidad de los actos de gobierno. El Estado no puede, en estos casos, utilizar software cuyo código fuente no esté públicamente disponible, sin violar principios constitucionales básicos relegados en la Constitución Política del Estado de Chile."[106]

En el mundo hay diferentes proyectos de ley que buscan recomendar el software libre, otorgando mayor puntaje a los programas con código fuente disponible en los concursos de la Administración. Pero este aún es un tema delicado. En Francia hay dos proyectos de ley, uno que pretende establecer premios y recomendaciones, y otro que pretende obligar a la Administración a trabajar con software abierto, que, al parecer, no tiene muchos visos de imponerse. Hay opiniones que abogan porque no se obligue a erradicar el software propietario de la Administración, sino que sólo se debería aconsejar la utilización del software abierto, así, "afirman que una ley de ese tipo sería una peligrosa arma de doble filo que impediría el uso de miles de programas, muchos de ellos necesarios y apetecibles, y que por otra parte se daría una razón estupenda a las grandes corporaciones para que alegaran discriminación."[107]

En concordancia con este análisis, podemos decir que las ventajas de la utilización de software libre pueden resumirse en:

- Contar con aplicaciones fáciles de modificar y adaptar a las necesidades de la Administración del Estado;

---

[105] Software Libre Chile. Software Libre en Chile. Misión del Estado [en línea] <http://www.softwarelibre.cl/drupal//?q =node/120> [consulta: 23 de marzo de 2006]

[106] Software Libre Chile. Software Libre en Chile. Misión del Estado [en línea] <http://www.softwarelibre.cl/drupal//?q =node/120> [consulta: 23 de marzo de 2006]

[107] Melisa Tuya. Software abierto software seguro [en línea] <http://www.baquia.es/com// 20010418/art00024.html> [consulta: 27 de septiembre de 2005]

- Poder obtener el apoyo de miles de programadores para la solución de problemas, teniendo un amplio campo de pruebas.

- Precio muy bajo o gratuito, incluso en las aplicaciones para estos sistemas.

Por su parte, podemos decir que las desventajas de la utilización de software libre pueden resumirse en:

- Escasez de soporte técnico certificado, aunque el calificado es abundante.

- No lo conoce mucha gente, por lo que normalmente requiere un periodo de aprendizaje y adaptación.

2.3.- Análisis de software ya desarrollado, propietario o libre.

2.3.1.- La auditoria informática.

Una forma de lograr software seguro es desarrollando auditorias informáticas, que se han definido como "la actividad consistente en la opinión profesional sobre si los sistemas de aplicación, recursos informáticos, planes de contingencia, etc. Presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que la han sido prescritas, como eficiencia, eficacia, economicidad."[108]

Otra forma de definirla ha sido como "la investigación, consulta, revisión, verificación, comprobación y obtención de la evidencia sobre un hecho acontecido o sistema establecido, según el desarrollo de las normas de aplicación, a través de la certificación del personal cualificado y acreditado al respecto."[109]

[108] Mario Piattini V y Emilio del Peso N. auditoria Informática, un enfoque práctico. Ed. RA-MA. Madrid. 2001. p. 4.
[109] Jordi Velazco D. y Luis Velazco M. auditoria de la protección de datos. Ed. Bosch. Barcelona, 2005. p.21

Finalmente, podemos entender como auditoria informática “la revisión de la propia informática y de su entorno, y ello no implica que haya que usar el ordenador (puede tratarse, por ejemplo, de una auditoria de la gestión de la informática, de desarrollo de aplicaciones...), aunque algunos entienden la auditoria informática como la auditoria de cuentas con ayuda de ordenadores (personales, sobre todo), que es una tendencia, pero que no responde al concepto que estamos tratando. Deberíamos tal vez hablar de auditoria EN Informática, como dicen en algunos países hispanoamericanos.”[110]

De esta manera, para la auditoria informática es una herramienta que sirve para detectar las fallas de seguridad.

Respecto de la normativa que fundamenta la ejecución de auditorias informáticas por parte de los órganos de la Administración del Estado en Chile, llama la atención la ausencia en la ley N° 19.628, sobre protección de los datos de carácter personal, de una referencia a la auditoria, a diferencia de la legislación española que en el artículo 17.1 del Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los Ficheros Automatizados que Contengan Datos de Carácter Personal, que expresamente establece la obligación de realizar una auditoria de seguridad, externa o interna, de los sistemas de información que contengan datos de carácter personal.

En el artículo 8°, inciso segundo del Decreto Supremo N° 83 de 2004, del Ministerio Secretaría General de la Presidencia, sobre seguridad y confidencialidad del documento electrónico, ya criticado, se establece como condición para que el órgano de la Administración del Estado pueda no cumplir con los atributos esenciales para la seguridad del documento electrónico que un análisis de riesgo lo estime innecesario. Llama poderosamente la atención que esta norma dé a las auditorias informáticas en seguridad el lugar de forma de excepción de las normas de seguridad del software, en vez de darles el carácter de control de cumplimiento de dichas normas.

[110] Emilio del Peso Navarro y Miguel Ángel Ramos González. Confidencialidad y seguridad de la información: La LOARTAD y sus implicancias socioeconómicas. Ed. Díaz de Santo S.A. Madrid, 1994. p 50.

Por su parte, el artículo 1 letra c) de la misma norma señala que cada órgano público deberán fijar las directrices mínimas de seguridad dentro de ella, en la que se debe incluir su reevaluación en forma periódica, a lo menos cada tres años. Desearíamos pensar que dicha reevaluación debiera tener entre sus elementos una auditoria informática.

Siguiendo a los profesores Jordi y Luis Velazco[111] esta disciplina, tiene como características fundamentales la objetividad, que se refiere principalmente a la información que se produce luego de la auditoria, señalándose que debe ser comprobable; la independencia; la documentación, que se refiere a los documentos o registros que el auditado debe entregar al auditor; la sistematización, que implica desarrollar la auditoria en virtud de un procedimiento estandarizado, tanto en su metodología como en su aplicación; y la periodicidad, que significa la aplicación constante de dicho procedimiento, en períodos de tiempo determinados.

Hemos dejado pendiente la explicación sobre la independencia de la auditoria informática porque estimamos que es de gran importancia para el tema que estamos comentando. "Como requisito básico para garantizar la objetividad, el auditor no debe tener vinculación alguna con los profesionales internos y/o externos que participan en el sistema sujeto a auditoria. Evidentemente esto supone que el propio auditor no puede asesorar en la implantación de aquello que posteriormente verificará."[112] Lo interesante de esta característica fundamental es que las normas nacionales que de una u otra forma se refieren a este tipo de prácticas no se explicitan las incompatibilidades que existen entre los auditores y los funcionarios o proveedores.

Ahora bien, como es evidente, la auditoria informática es sólo un modo en que la Administración del Estado puede evaluar la seguridad del software con que funciona, ya que, como hemos venido diciendo, el software propietario imposibilita a la

[111] Jordi Velazco D. y Luis Velazco M. auditoria de la protección de datos. Ed. Bosch. Barcelona, 2005. p.24
[112] Jordi Velazco D. y Luis Velazco M. auditoria de la protección de datos. Ed. Bosch. Barcelona, 2005. p.24

Administración del Estado saber con certeza la forma en que este funciona y qué tipo de operaciones realiza, con lo ningún órgano público podría detectar la instalación de posibles puertas traseras o fallas del programa que permitan el acceso de intrusos a la información que maneja el Estado. Por esto, la auditoria informática sería una forma de conocer los posibles fallos de seguridad del software de modo de no vulnerar el derecho de autor sobre el software, que por lo mismo, es una herramienta muy restringida como solución de los problemas, sino que es una herramienta de detección, que en la mayoría de los casos, debe venir acompañada de métodos de solución para las fallas detectadas, que en este caso son muy difíciles de conseguir, ya que las licencias de software propietario impide realizarle modificaciones.

Tratándose de software cuyo Código Fuente es conocido, puede efectuarse sobre él la denominada Auditoria de Código Fuente, también conocida como RTFS (“Read the fine source”). Esta auditoria se desarrolla en dos partes, primero consiste en leer el código fuente cuidadosamente, detallando y documentando las fallas de seguridad provocadas por malas prácticas de programación, y en segundo lugar, volver a realizar la lectura, pero buscando una detección profunda y detallada de las fallas de seguridad intrínsecas al diseño e implementación del software.

Esta auditoria no presentaría problemas respecto al derecho de autor del software libre, ya que al ser público su Código Fuente y permitida su modificación, la Administración del Estado se encuentra autorizada expresamente para efectuarla, por lo tanto, existe esta herramienta muy útil para asegurar el software. E incluso, yendo más allá, podemos estimar que es una obligación para el Estado realizar este tipo de auditorias al software libre que posea en el entorno del Gobierno Electrónico, como herramienta indispensable para lograr la mayor eficiencia y eficacia.

Otra forma de auditoria informática, útil tanto para software libre como para software propietario, son las denominadas Pruebas de Caja Negra, que es una forma muy útil para detectar fallas de seguridad en software sobre los que no se tiene mayor información ni son susceptibles de ingeniería inversa, que ya analizaremos.

Las Pruebas de Caja Negra consisten en tratar al software como una caja negra, esto es “un dispositivo que acepta ciertas entradas y produce un conjunto de salidas”. Así, los auditores modificarán las entradas normales que reconoce el software, o modificarán las condiciones ambientales en las que este opera. Así, si las salidas o respuestas del programa son las que se esperarían en condiciones normales, se determinará que no existen problemas de seguridad, pero si no es así, o sea, el software no está haciendo aquello para lo que fue creado, el software sería vulnerable.

El problema aquí está dado nuevamente por la capacidad de modificar la programación del software propietario, limitado por el derecho de autor.

2.3.2.- La ingeniería inversa.

“Se llama ingeniería inversa al intento de descubrir el diseño a partir de la máquina, en contraste con la ingeniería tout court que es el intento de producir la máquina a partir del diseño.”[113] Este es un concepto que nace principalmente en los tiempos de la guerra fría, aunque es una disciplina que se practica desde los tiempos antiguos.

El objetivo de la ingeniería inversa es obtener información técnica a partir de un producto al que se tenga acceso, con el fin de determinar de qué está hecho, qué lo hace funcionar y cómo fue fabricado. El software es uno de los productos que más es sometido a este tipo de técnicas. Pero este término no sólo se aplica al software. Así pues se considera ingeniería inversa también al estudio de todo tipo de elementos, por ejemplo equipos electrónicos, mecánicos, etcétera, siempre y cuando el resultado de dicho estudio repercuta en el entendimiento de su funcionamiento.

Este método es denominado ingeniería inversa porque avanza en dirección opuesta a las tareas habituales de ingeniería, que consisten en utilizar datos técnicos para elaborar un producto determinado, y supone profundizar en el estudio de su

[113] Claudio Gutiérrez. Ingeniería Inversa [en línea] <http://claudiogutierrez.com/NuevoHumanismo/ingenieria_inversa.html> [consulta: 28 de septiembre de 2005]

funcionamiento, hasta el punto de que podemos llegar a entender, modificar y mejorar dicho modo de funcionamiento.

La ingeniería inversa es una herramienta óptima en el caso de software relativamente pequeño y no muy complejo, y en su desarrollo, se deben tener en cuenta dos conceptos básicos, la depuración y el desensamblaje. “La depuración exige monitorear activamente la ejecución del software para comprender sus funciones y como se ejecutan. Los desarrolladores de software regularmente usan esta técnica para encontrar y reparar bugs (relacionados con la seguridad o no) cuando un programa se comporta de una manera incorrecta o cuando un bug se manifiesta durante la ejecución del programa, pero no se han encontrado problemas con el código fuente… Los cazadores de bugs aplican la misma idea. Ellos seleccionan entradas para el programa y siguen cada posible camino en la ejecución.” [114] Por su parte, “el ‘desensamblado’ exige obtener y entonces analizar código fuente desde una imagen ejecutable del producto de software.”[115]

La pregunta que cabe hacerse, es ¿Cuál es la diferencia con la auditoria de código fuente? Pues, el profesor Arce nos explica que “el ‘Desensamblado’ produce código fuente en ensamblador, el lenguaje de programación de bajo nivel para la arquitectura del microprocesador del software. Sin embargo, el código puede ser muy complejo y generalmente difiere del código fuente de lenguaje de alto nivel que produjo la imagen ejecutable (aunque desempeña las mismas funciones). Además, la entrada de los miembros del equipo de desarrollo es menos importante, porque ellos desarrollaron el software en un lenguaje de alto nivel y por eso tienen menos comprensión de las

[114] Iván Arce. Cacería de bugs: Las siete vías del samurai de la seguridad. Traducción de Luis Valencia Reyes [en línea] <http://www.ewh.ieee.org/r9/guadalajara/boletin/diciembre2002.pdf> [consulta: 11 de noviembre de 2005]
[115] Iván Arce. Cacería de bugs: Las siete vías del samurai de la seguridad. Traducción de Luis Valencia Reyes [en línea] <http://www.ewh.ieee.org/r9/guadalajara/boletin/diciembre2002.pdf> [consulta: 11 de noviembre de 2005]

características del software, sus funciones y componentes, relacionados con el código desensamblado."[116]

Otra forma de ingeniería inversa es la denominada ingeniería inversa de tráfico de red. "Cuando el código fuente no está disponible, o cuando la tecnología objetivo es grande o compleja (como por ejemplo un sistema operativo propietario) o interactúa con otros componentes de red, los cazadores de bugs deben comprender las interacciones globales de la tecnología e identificar problemas en ellas. Para hacer esto, puede utilizarse un sniffer –un programa que captura todos los paquetes que viajan por la red a través de un cable- para detectar posibles fallas en el mecanismo de comunicación."

"Los cazadores de bugs no necesariamente requieren conocer los protocolos de comunicación involucrados. Modificar y repetir el tráfico capturado o generar tráfico espurio pueden revelar bugs de seguridad. La búsqueda de bugs basada en el análisis de la comunicación entre componentes típicamente requiere un experto cazador de bugs que comprende los protocolos de red y su utilización en escenarios del mundo real. Requiere menos experiencia de bajo nivel en la plataforma o nivel del sistema operativo."[117]

Como ya venimos diciendo respecto del software propietario, las licencias que tanto los particulares como la Administración del Estado deben suscribir para su uso imposibilitan el ejercicio de este tipo de prácticas. Por su parte, respecto del software libre, la ingeniería inversa no es necesaria, dado que su código fuente está ya disponible para cualquier usuario, permitiendo todas y cada una de las actividades e intervenciones en el software con el objetivo de incrementar su seguridad.

---

[116] Iván Arce. Cacería de bugs: Las siete vías del samurai de la seguridad. Traducción de Luis Valencia Reyes [en línea] <http://www.ewh.ieee.org/r9/guadalajara/boletin/diciembre2002.pdf> [consulta: 11 de noviembre de 2005]

[117] Iván Arce. Cacería de bugs: Las siete vías del samurai de la seguridad. Traducción de Luis Valencia Reyes [en línea] <http://www.ewh.ieee.org/r9/guadalajara/boletin/diciembre2002.pdf> [consulta: 11 de noviembre de 2005]

Respecto del software propietario, la ingeniería inversa puede estimarse como una violación al derecho de autor. ¿Podría la Administración del Estado o un particular hacer ingeniería inversa sobre el software que utiliza? En primer término, respecto de la ley de delitos informáticos, nos parece que al tenor de los tipos penales ahí establecidos, que atienden principalmente a la intencionalidad y resultado de dicha acción, no habría delito informático si no se realiza "indebidamente" ni "maliciosamente", esto es, sin la intención positiva de conocer información reservada o causar daño en los sistemas de tratamiento de información. Sin embargo, respecto del derecho de autor sobre el software el asunto es distinto, pues, al ser la ingeniería inversa expresamente rechazada en los contratos de licencia de software propietario, debemos entender que sea un particular, o sea la Administración del Estado quien la realice, siempre será ilícita.

El Estado como garante del bien común, los principios de eficiencia y eficacia Administrativa y la normativa general y específica aplicable al gobierno electrónico, que como vimos, obligan a la Administración del Estado a mantener software seguro, son afirmaciones que quedan en entredicho frente al derecho de autor del software que utiliza el Estado, pues, conociendo de fallas de seguridad en dichos software, el Estado queda atado de manos a la voluntad del proveedor de dicho software para la reparación de dichos daños.

En esto radica la importancia de los contratos de adquisición y del tipo de software que se utilice, pues, de encontrarse prohibidas estas maniobras, al Estado no le quedaría otra forma de actuar apegada a la Constitucionalidad y legalidad que proceder respecto del derecho de autor por medio de un procedimiento de expropiación, según lo dispone el artículo 19 Nº 24 de la Constitución Política de la República, que asegura a todas las personas el derecho de propiedad en sus diversas especies sobre toda clase de bienes corporales o incorporales, donde se incluyen los derechos de autor, con todas las implicancias que eso tendría, en especial, la falta de interesados de proveer al Estado de software propietario ante los llamados a licitación, por la desconfianza que esto generaría ante los proveedores.

CONCLUSIONES

La Administración del Estado está compuesta por diversos organismos y servicios que están jerárquicamente organizados, y que someten su funcionamiento a un órgano supremo, singular y central. Es este el modelo que existe en Chile, siendo este órgano superior, el Jefe de Estado, es decir, el Presidente de la República. De este modo, según el mandato constitucional y legal la administración del Estado la ejerce el Presidente de la República, quien será asistido en su ejercicio por los Ministerios, Subsecretarías, Intendencias, Gobernaciones, Direcciones y Servicios Públicos, como la Tesorería General de la Republica, el Servicio de Impuestos Internos, el Servicio de Registro Civil e Identificación, los Servicios de Salud, las Fuerzas Armadas, Carabineros de Chile, la Policía de Investigaciones, Gendarmería, etc.

Dadas sus especiales funciones y tareas, los servicios públicos deben cumplir sus labores e interactuar, más algunos, menos otros, con los particulares de manera regular y continua, siempre en búsqueda de lograr la mayor realización espiritual y material posible de las personas, que es su cometido fundacional, consagrado en el artículo 1º de la Constitución Política de la República.

Para el cabal cumplimiento de su obligación, toda actuación de la Administración del Estado debe ceñirse estrictamente a los principios que consagran la Constitución y las leyes. Los principios de eficiencia y eficacia son precisamente directrices inexcusables para la Administración. Así, la eficiencia puede caracterizarse como la virtud y facultad para obtener un resultado determinado utilizando de la mejor manera los recursos escasos que se poseen, mientras que la eficacia es la aptitud que tienen las acciones realizadas para obtener el resultado esperado.

Las Tecnologías de la Información y Comunicación son herramientas que permiten a la Administración del Estado lograr niveles de eficiencia y eficacia nunca antes vistos en la entrega, recolección y administración de información y en la comunicación con los

particulares y entre la Administración misma, siendo canales abiertos las 24 horas los 365 días del año para satisfacer las necesidades de los particulares.

Así, al uso de TIC por parte de los órganos de la Administración del Estado para mejorar cualitativamente los servicios e información por ella ofrecida a los ciudadanos, aumentar la eficiencia y eficacia de la gestión pública e incrementar sustantivamente la transparencia del sector público y la participación ciudadana mediante el diálogo virtual, se le ha denominado Gobierno Electrónico, Gobierno Digital o E-Government.

Sin embargo, el sólo uso de las TIC en el ámbito público no produce una mejora en la eficiencia y eficacia, sino que este logro depende de la forma y las características que tengan las herramientas con que se implemente, por lo que es necesario que, entre muchos otros factores, el software con el que se haga sea seguro, esto es, que siga funcionando correctamente frente a cualquier ataque, que dé acceso a la información que utiliza sólo a usuarios autorizados, que resguarde los datos que maneja y los proteja frente a manipulación consciente o inconsciente de los usuarios y que su disponibilidad esté siempre garantizada.

Así, a primera vista, estando obligada la Administración del Estado de manera imperativa por los principios de eficiencia y eficacia, y existiendo herramientas que permiten su estricto cumplimiento, el Estado está, en primer lugar, obligado a implementar Gobierno Electrónico, y no sólo eso, sino que también se encuentra obligado a que aquellas herramientas efectivamente sirvan para hacer sus labores de manera más eficiente y eficazmente, para lo cual el software debe ser seguro.

Respecto de la libertad que se le otorga a cada órgano de la Administración del Estado para determinar su propia política que fije las directrices generales que orientan la materia de seguridad, establecida en los artículos 11 y 37 letra a) del D. S. Nº 83 de 2004 del MINSEGPRES, nos parece que la visión que fundamenta esta norma, esto es, que los distintos órganos de la Administración del Estado tienen distintos requerimientos de seguridad, ha sido tomada en un sentido amplísimo, pues deja en manos de cada órgano la definición de seguridad del documento electrónico, sus

objetivos globales, alcance e importancia, la difusión de sus contenidos al interior de la organización y una reevaluación periódica a lo menos cada tres años, materias todas que deberían quedar centralizadas en un órgano específico y que uniforme aquellos criterios básicos de seguridad. La uniformidad de los criterios básicos de seguridad del software dentro de la Administración del Estado traería entre sus consecuencias, un uso más eficiente de los recursos y un marco jurídico claro dentro del cual los entes públicos pueden desenvolverse.

Es en virtud de este mismo fundamento que la normativa específica sobre la materia pareciera señalar que la obligación del Estado de dar seguridad al software de Gobierno Electrónico es relativa, no sin razón en algunos casos, permitiendo a la Administración del Estado utilizar software inseguro en el desarrollo de sus labores por medios electrónicos. Como ejemplo paradigmático de esto encontramos el artículo 8º inciso segundo del D. S. Nº 83 de 2004 del MINSEGPRES, donde se materializa de mejor forma la íntima relación que existe entre la seguridad del software y la eficiencia y eficacia, al permitir que los órganos de la Administración del Estado mantengan software seguro en consideración de factores de riesgo y factores de costo/beneficio, los que el jefe del servicio podrá invocar mediante resolución fundada basada en un estudio al efecto

De esta norma podemos concluir, en primer término, que ningún órgano de la Administración del Estado está facultado para tener software que no cumpla con las características de seguridad recién indicadas - esto es, que siga funcionando correctamente frente a cualquier ataque, que dé acceso a la información que utiliza sólo a usuarios autorizados, que resguarde los datos que maneja y los proteja frente a manipulación consciente o inconsciente de los usuarios y que su disponibilidad esté siempre garantizada - excepto si efectivamente ha realizado un estudio de riesgo o costo/beneficio y este ha sido invocado por el jefe del servicio en resolución fundada. Cualquier actuación en otro sentido configura claramente una violación a los principios de eficiencia y eficacia administrativa, además de ser causal de responsabilidad para el funcionario por falta de probidad en el ejercicio de su cargo.

La segunda conclusión derivada de esta norma se refiere a la dificultad que tendría el jefe del servicio para fundamentar su decisión de utilizar software esencialmente inseguro. Esto debido a que toda información que maneja la Administración del Estado es pública, excepto si se trata de información que pueda encuadrarse dentro de la muy calificada excepción establecida en el artículo 13 de la LOCBGAE o que sea información de carácter personal. Además, y como lo reconocen los Decretos Supremos del MINSEGPRES, la información es fundamento esencial para la toma de decisiones, tanto para los particulares como para la Administración misma, por lo tanto, el Estado, como mayor ente poseedor de información relevante, debe tener siempre a disposición de los interesados la información por ella ofrecida, esta debe ser siempre fidedigna y debe especialmente mantener abiertos los canales de comunicación con los particulares y entre sí.

Sin embargo, es entendible que existan órganos de la Administración del Estado que estimen que la posibilidad de ser víctimas de incidentes de seguridad sea baja, pero nos parece que la única conclusión atendible para permitir la mantención de software inseguro sería que el estudio de costo/beneficio determine que por las características que tiene la información que manejan, sea más económico soportar la responsabilidad económica que significaría para el Estado los daños que la fuga, modificación, eliminación o falta de disponibilidad de aquella información produzca que el cumplimiento de aquella premisa básica según la cual el Estado debe mantener la información que maneja en software seguro.

Por lo tanto, podríamos pensar que aquellos órganos de la Administración del Estado que manejan información de carácter personal o aquella que debe mantenerse en reserva en virtud de la ley, podrían tenerla en forma insegura, lo que a todas luces es incongruente con el fin del Estado, esto es, el Bien Común, y con los principios de eficiencia y eficacia administrativas. Así, creemos que estos órganos no pueden, en ningún caso, y bajo ninguna circunstancia tener dicha información en software inseguro.

Es indudable que la aplicación que da el D. S. Nº 83 de 2004 a la NCh2777 es un paso importantísimo en materia de seguridad de software, no es menos cierto que, lamentablemente, la forma en que esto se hizo trae aparejado algunos problemas. El primero es que la NCh2777 está desarrollada y dirigida principalmente a organismos privados, y por lo mismo, que se haya dado aplicación sin mayores indicaciones a este respecto hace que el énfasis esté puesto en la seguridad del acceso a la información, siendo que en el sector público la mayor preocupación debiera estar dada por la disponibilidad y certeza de la información, debiendo dar libre acceso, salvo las excepciones señaladas en la LOCBGAE. Otro problema es que la NCh2777 trata de la seguridad de la información contenida en cualquier tipo de soporte o entorno, no sólo al digital, por lo que muchas veces se hace difícil conciliar el tenor literal de la Norma Chilena con la aplicación que el D. S. le da, esta es, restringida únicamente a la seguridad del documento electrónico. Finalmente, es también perjudicial el hecho de que el D. S. da aplicación a la NCh2777 de forma segregada, cercenándola en sus contenidos y quitándole en algunos temas sensibles la coherencia que tiene la Norma Chilena en su integridad.

Ahora bien, ante la pregunta planteada desde un principio, entendiendo que el principio de Responsabilidad del Estado es la forma que da nuestra legislación nacional para dar vida y hacer exigible por los particulares el resto de los principios con reconocimiento constitucional y legal, como la eficiencia y la eficacia: ¿Debe responder el Estado por los daños que se produzcan derivados de la mantención de software inseguro en el ámbito del Gobierno Electrónico?, la respuesta, por fuerza debe ser afirmativa. Y ante la subsecuente pregunta sobre los casos en que ello debe ocurrir, la respuesta es en todos.

Esto debido a que si atendemos a la teoría de la responsabilidad objetiva del Estado, con la sola producción del daño derivado de mantener información en software inseguro, el Estado debe responder patrimonialmente ante el particular afectado. Ahora, si se atiende a la teoría de la responsabilidad subjetiva del Estado por falta de servicio, la respuesta debe ser también afirmativa, ya que la actuación alejada de los principios de eficiencia y eficacia, que fundan la obligación del Estado de tener

software seguro, configuran precisamente la falta del servicio, al ejercer el órgano público sus funciones de mala forma.

Muy ligado con esto, la falta del servicio como la prestación tardía, no eficaz o la falta de ella, se encuentra la característica de la normativa de Gobierno Electrónico enfocada a la reparación de las fallas de seguridad en forma reactiva, ya que aquello implica precisamente prestar el servicio de forma tardía. Es por esto también que la Administración del Estado debe bogar por la implementación desde ya de software seguro, cumpliendo con su mandato de satisfacer necesidades de forma regular y continua.

Por su parte, el funcionario público, que es responsabilizado expresamente en la normativa analizada por la seguridad de los documentos, registros, repositorios electrónicos, etcétera, debe responder en virtud de lo establecido en el Estatuto Administrativo y sólo en caso que su actuar sea de aquel que fundamenta una sanción. Pero respecto a su responsabilidad pecuniaria, derivada de la facultad que tiene el Estado de repetir el monto de lo indemnizado contra el funcionario autor del daño, debemos concluir que aquello sólo sería posible cuando las fallas de seguridad se hayan producido por la negligencia del funcionario, ya que de producirse por otros motivos, como la falta de presupuesto o incluso en cumplimiento de sus funciones, no cabría la repetición de lo pagado.

Así, el único modo por el cual la Administración del Estado puede hacer uso de software para cumplir cabalmente su rol de guardián y garante del registro público es por medio de la utilización de programas cuya licencia le conceda, sin limitación alguna, ejecutar, estudiar, corregir, mejorar, ampliar y adaptar el programa de acuerdo a sus necesidades, tanto del servicio como de seguridad, y no a las del proveedor, que son precisamente aquellas facultades que restringen las licencias de software propietario.

En Chile, el Estado sólo puede adquirir software de las formas que muy regladamente establece la Ley de bases sobre contratos administrativos de suministro

y prestación de servicios, pudiendo adquirir, principalmente dos tipos de software, libre y propietario.

A pesar que la ley de bases sobre contratos administrativos de suministro y prestación de servicios se refiere expresamente a la adquisición de software y sólo a la cesión del derecho de uso de estos últimos, característica esencial de la adquisición de software propietario, aquello no obsta que el Estado pueda adquirir software cuya licencia le otorgue más facultades, ya que la enunciación legal no es taxativa. Sin embargo, sería de gran utilidad explicitar en aquella ley que el Estado está facultado a adquirir software que le otorgue más libertades que el uso.

La utilización de software libre es una tendencia que ha ido tomando fuerza en otros países, y a la luz de lo expuesto pareciese que en Chile también hay buenas razones para hacerlo. No obstante aquello, deberán ser las autoridades quienes determinen caso a caso si para la actividad específica que se busca cumplir puede ser más útil un software propietario que uno libre. Lo que no debe nunca dejarse de lado es la seguridad, pues, por más que el software propietario sea útil específicamente para la actividad que se pretende ejercer, si este no es seguro, no es ajustada a derecho su adquisición, salvo la muy excepcional situación a que se refiere el artículo 8º inciso segundo del D. S. Nº 83 de 2004 del MINSEGPRES.

Aunque en Chile se han hecho esfuerzos para determinar la cantidad y calidad del gasto que se hace en Gobierno Electrónico, ellos aún son deficientes. Sin embargo, la premisa básica ante la cual debemos entender esta materia es que más gasto no significa más seguridad. En otras palabras, no necesariamente debe el Estado desembolsar cantidades de dinero insostenibles en el tiempo para tener software seguro, sino que lo importante es hacer un uso inteligente y eficiente, de los recursos. Así, el Estado debe mantener software seguro a cualquier costo que permita mantener el estándar de eficiencia, pero que en todo caso puede ser, si se implementa una política en tal sentido, relativamente bajo.

Ahora bien, respecto de las acciones que pueden realizar los particulares en torno a detectar y denunciar fallas de seguridad del software, debemos decir que no necesariamente esas acciones podrán ser sancionadas penalmente como delito informático, ya que aquella ley atiende, por una parte, a la intencionalidad del sujeto al vulnerar los sistemas de seguridad del software y, por otra, a los resultados dañosos que esa vulneración produzca en el sistema de tratamiento de información.

Por su parte, las acciones deliberadas para dañar o modificar información digital del Estado o para conocer indebidamente información contenida en los sistemas de gobierno electrónico, serían constitutivas de delito informático, según la ley que tipifica figuras penales relativas a la informática. En este mismo sentido, debemos concluir que dada la antigüedad de dicha ley, nos parece adecuado en torno a proteger la información contenida en el software del Estado y evitar que las personas siquiera intenten vulnerar su seguridad, establecer una calificación de los delitos ahí señalados, aumentando las penas a aquellas acciones que tengan como objeto la información que el Estado maneja por medio de software.

Pero respecto de las mismas acciones, sean hechas por particulares o por el Estado mismo, puede ser, dependiendo de la licencia respectiva del software, que dadas las limitaciones que ellas imponen, y al tipo de acción que se realice, podrían dar lugar a alguna de las infracciones establecidas en la ley de propiedad intelectual, como por ejemplo hacer ingeniería inversa. Esto, aunque la intención sea detectar y alertar al Estado de las fallas de seguridad. Recalcamos aquí que este problema se produce exclusivamente respecto del software propietario y que, por el contrario, también existen formas, como la auditoria informática, en que pueden detectarse las fallas de seguridad sin violentar los derechos de los autores del software.

En definitiva, la obligación del Estado como garante del Bien Común y ejecutor del Gobierno Electrónico debe superponerse a los intereses económicos, y debe ser tomada en cuenta al momento de contratar uno u otro tipo de software. Aquí no nos estamos refiriendo al pago de licencias ni haciendo una defensa de la utilización del software libre por parte del Estado, sino que tomando en cuenta que la normativa que

rige al Estado la restringe enormemente en materia económica y tecnológica, deben respetar normas imperativas muy estrictas. Esto se produce debido a que el fin del Estado es diverso, e incluso muchas veces contrapuesto al de los particulares, y por lo tanto, en sus acciones, incluidas las formas de obtener software seguro, debe tener siempre presente estas diferencias.

BIBLIOGRAFÍA

ARCE, Iván. Cacería de bugs: Las siete vías del samurai de la seguridad. Traducción de Luis Valencia Reyes [en línea] <http://www.ewh.ieee.org/r9/guadalajara/boletin/diciembre2002.pdf> [consulta: 11 de noviembre de 2005]

ARRIAGADA, Anita. Sitios de gobierno están a merced de los hackers [en línea] Portal Terra. cl. 12 de septiembre de 2005 <http://www.terra.cl/tecnologia/index.cfm?Id_cat=1719&pagina=1&id_reg=534884&accion=secretos> [consulta: 12 de septiembre de 2005]

CANO, Jeimy J. Breves reflexiones sobre la programación segura [en línea] <http://www.virusprot.com/Art42.html> [consulta: 15 de noviembre de 2005]

CARRACEDO GALLARDO, Justo A. Provisión de protocolos de anonimato para la protección de la privacidad y el desarrollo de la democracia electrónica en las comunicaciones mediante computadores. En: HERIBERTO CAIRO CAROU (Ed.). Democracia Digital, Límites y Oportunidades. Madrid. Ed. Trotta, 2002. pp. 31-43.

CARRANZA TORRES, Javier. La Promoción del Desarrollo de Tics en los Gobiernos Locales. El Gobierno Electrónico Desde la Visión del Sujeto [en línea]. Comunidad Virtual de Gobernabilidad Desarrollo Humano e Institucional <http://www.gobernabilidad.cl/modules.php?name=News&file=article&sid=873> [consulta: 22 de noviembre de 2005]

COLOMINA P., Otto, FLORES R., Francisco, MORA P., Jerónimo. Introducción a la Informática para Juristas. Alicante. Ed. Club Universitario. 1997. 157 p.

DEFINICIÓN.ORG. Definición de Código Fuente [en línea] <http://www.definicion.org/codigo-fuente> [consulta: 30 de abril de 2006]

DIRECCIÓN de Presupuesto (DIPRES) – Ministerio de Hacienda. Informe de Cuantificación del Gasto en Gobierno Electrónico año 2003, 2005, 23 p.

FUNDACIÓN Iberoamericana para la Gestión de la Calidad (FUNDIBEQ). Boletín Electrónico Aprender de los Mejores – Octubre Nº 5 [en línea] <http://www.iberpymeonline.org/Documentos/AprenderMejores5.pdf> [consulta: 23 de agosto de 2007]

GARCÍA PÉREZ, Pablo. Principios Básicos de Desarrollo Seguro [en línea] <http://www.germinus.com/sala_prensa/articulos/ppos%20basicos%20desarrollo%20seguro.pdf> [consulta: 23 de marzo de 2006]

GRIMALDOS PARRA, José J. Manual Básico de Uso Guadalinex Edu [En línea] <http://www.juntadeandalucia.es/averroes/manuales/guadaconceptos.html> [Consulta: 16 de octubre de 2006]

GRUPO de Acción Digital. Agenda Digital 2004-2006. Segunda Edición, 2004. 60 p.

GUTIÉRREZ, Claudio. Ingeniería Inversa [en línea] <http://claudiogutierrez.com/NuevoHumanismo/ingenieria_inversa.html> [consulta: 28 de septiembre de 2005]

HUEPE ARTIGAS, Fabián Andrés. Responsabilidad del Estado, Falta de Servicio y Responsabilidad Objetiva en su Actividad Administrativa. Santiago – Chile. Instituto Chileno de Derecho Administrativo. 2004. 184 p.

JIJENA LEIVA, Renato. Procedimientos Administrativos y Gobierno Electrónico: el impacto de las tecnologías en el Derecho Público Chileno [en línea] Uniacc e- campus <http://www.ecampus.cl/Textos/ derecho/jijena/jijena.htm> [consulta: 28 de septiembre de 2005]

LUCAS DURAN, Manuel. El Acceso a los Datos en Poder de la Administración Tributaria. Pamplona. Ed. Aranzadi, 1997. 289 p.

MORAGA K., Claudio. Principios con reconocimiento legal a que debe observancia la Administración del Estado. Apuntes de clases Facultad de Derecho Universidad de Chile (primer semestre 2002). 17 p.

MOYA GARCÍA, Rodrigo: El Procedimiento Administrativo Electrónico en Chile. En su: El Procedimiento Administrativo Electrónico, Los desafíos de su implementación, Materiales para el Magíster en Derecho de la Informática y las Telecomunicaciones, Escuela de Graduados, Facultad de Derecho, Universidad de Chile.

NOGUEIRA A., Humberto; CUMPLIDO C., Francisco. Derecho Político, Introducción a la Política y Teoría del Estado. Instituto Chileno de Estudios Humanísticos. Santiago, 1987. 329 p.

PALAZZI, Pablo A. Delitos Informáticos. Buenos Aires. Editorial Ad-Hoc, 2000. 272p.

PANTOJA BAUZÁ, Rolando. El Derecho Administrativo. Clasicismo y Modernidad. Santiago de Chile. Ed. Jurídica de Chile. 1994. 274 pp.

PERALTA CÁCERES, Rodrigo. La seguridad no ha sido abordada como un tema de Estado [en línea] Portal Terra. cl. 13 de septiembre de 2005 <http://www.terra.cl/ tecnologia/index.cfm?accion=bits&id=537031> [consulta: 13 de septiembre de 2005]

PESO NAVARRO, Emilio del; RAMOS GONZÁLEZ, Miguel Ángel. Confidencialidad y seguridad de la información: La LOARTAD y sus implicancias socioeconómicas. Ed. Díaz de Santo S.A. Madrid, 1994. 348 p.

PIATTINI VEITHUIS, Mario Gerardo; PESO NAVARRO, Emilio del. Auditoria Informática, un enfoque práctico. Ed. RA-MA. Madrid. 2001. 660 p.

PROYECTO de Reforma y Modernización del Estado - Ministerio Secretaría General de la Presidencia. Agenda Gobierno Electrónico 2002-2005. Santiago de Chile, 2002. 36 p.

PROYECTO de Reforma y Modernización del Estado – Ministerio Secretaría General de la Presidencia. Chiecompra genera importantes ahorros al presupuesto 2004 [en línea] Portal Modernización.cl. 6 de octubre de 2003 <http://www.modernizacion.cl /1350/article-48817.html> [consulta: 23 de marzo de 2006]

PROYECTO de Reforma y Modernización del Estado - Ministerio Secretaría General de la Presidencia y Programa de Modernización de la Gestión Pública - Departamento de Ingeniería Industrial - Universidad de Chile. Gobierno Electrónico en Chile: Estado del Arte. Santiago de Chile, 2003. 134 p.

SCHUSTER PINEDA, Felipe. Programas de Computación/software [en línea] <http://www.universidadvirtual.cl/downloads/laadaptacion.ppt> [consulta: 20 de abril de 2006]

SERVICIO de Impuestos Internos. SII Internet. Hacia un Gobierno Electrónico [en línea] <http://www.sii.cl/sii_internet/sii_internet.htm> [consulta: 20 de noviembre de 2005]

SILVA BASCUÑÁN, Alejandro. Tratado de Derecho Constitucional. Tomo I, Principios. Ed, Jurídica de Chile, Santiago de Chile, 1963. 549 p.

SILVA CIMMA, Enrique. Derecho Administrativo Chileno y Comparado; El Servicio Público. Ed. Jurídica de Chile, Santiago de Chile, 1995. 323 p.

SOCIEDAD chilena de Derecho de Autor. Legislación Chilena sobre Propiedad Intelectual. Colección de textos legales y resoluciones. Santiago de Chile, 2001. 309 p.

SOFTWARE libre Chile. Software Libre en Chile. Misión del Estado [en línea] <http://www.softwarelibre.cl/drupal//?q=node/120> [consulta: 23 de marzo de 2006]

THE GNU Project. La definición de Software Libre [en línea] <http://www.gnu.org/philosophy/free-sw.es.html> [consulta: 28 de marzo de 2006]

TUYA, Melisa. Software abierto software seguro [en línea] <http://www.baquia.es/com//20010418/art00024.html> [consulta: 27 de septiembre de 2005]

VALERO TORRIJOS, Julián. El régimen jurídico de la e-Administración. El uso de medios informáticos y telemáticos en el procedimiento administrativo. Granada. Editorial Comares, 2004. 224 p.

VELAZCO DOBATO, Jordi; VELAZCO MASSIP, Luis. Auditoria de la protección de datos. Ed. Bosch. Barcelona, 2005. 225 p.

VERA QUILODRÁN, Alejandro. Delito e Informática: La informática como fuente de delito. Santiago. Editorial Jurídica La Ley, 1996. 279 p.

WORLD BANK Group. A definition of e-government [en línea] <www.worldbank.org/publicsector/egov/definition.htm> [consulta: 28 de noviembre de 2005]