UNIVERSIDAD SAN FRANCISCO DE QUITO USFQ

Colegio de Ciencias Sociales y Humanidades

Los efectos del Dilema en la Soberanía del Ecuador de temas de Seguridad Nacional e Individual de Medios Informáticos

Artículo Académico

Samuel Andrés Tejada Cedeño

Relaciones Internacionales

Trabajo de titulación presentado como requisito
para la obtención del título de
Licenciado en Relaciones Internacionales

Quito, 12 de mayo de 2016

UNIVERSIDAD SAN FRANCISCO DE QUITO USFQ

COLEGIO DE CIENCIAS SOCIALES Y HUMANIDADES

HOJA DE CALIFICACIÓN
DE TRABAJO DE TITULACIÓN

Los efectos del Dilema en la Soberanía del Ecuador de temas de Seguridad Nacional e Individual de Medios Informáticos

Samuel Andrés Tejada Cedeño

Calificación: _____

Nombre del profesor, Título académico: Tamara Townsell, Ph.D.

Firma del profesor: _____

Quito, 12 de mayo de 2016

Derechos de Autor

Por medio del presente documento certifico que he leído todas las Políticas y Manuales de la Universidad San Francisco de Quito USFQ, incluyendo la Política de Propiedad Intelectual USFQ, y estoy de acuerdo con su contenido, por lo que los derechos de propiedad intelectual del presente trabajo quedan sujetos a lo dispuesto en esas Políticas.

Asimismo, autorizo a la USFQ para que realice la digitalización y publicación de este trabajo en el repositorio virtual, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

Firma del estudiante: _____

Nombres y apellidos: Samuel Andrés Tejada Cedeño

Código: 00113331

Cédula de Identidad: 0916270069

Lugar y fecha: Quito, mayo de 2016

Dedicado

A mis queridos padres Leopoldo y Lourdes que con trabajo, paciencia y amor me apoyaron durante todo el tiempo que dedique a cumplir esta meta. A mi compañera y futura esposa Ina que me ayudó a recordar el propósito en la vida.

Por ellos y para ellos……..muchas gracias.

Agradecimiento

Agradezco a Dios en primer lugar que me dio la fuerza todos los días para superarme. Por su infinito amor al bendecirme con una familia amorosa.

A mis padres Leopoldo y Lourdes por brindarme la mejor educación posible, soy muy bendecido. A mis hermanos Diego y Valeria por su apoyo incondicional. A mi prometida y amada Ina, gracias por la paciencia y el amor incondicional.

A mis profesores que me acompañaron en cada proceso durante los cuatro años que curse por la Universidad San Francisco de Quito. El conocimiento que me brindaron es invaluable, lo usaré sabiamente.

A cada persona y amigo que tuve el placer de conocer en la Universidad San Francisco de Quito, ustedes han hecho que estos cuatro años sean maravillosos.

Gracias a todos.

RESUMEN

La soberanía es un principio configurado de aplicaciones multidimensionales como estatales e individuales que son afectadas por el dilema en la conceptualización de las mismas. Recientemente, Ecuador ha contratado a empresas privadas de telecomunicación para la creación de bases de datos a nivel nacional. El control de la base de datos generará una amenaza en la seguridad nacional, en vez de protegerla. Esto desemboca en un dilema conceptual de soberanía en temas de seguridad. Por lo tanto, se identifica por medio de la cuantificación de tecnología (ej. número de satélites, programas cibernéticos), los efectos que tiene. Uno de los efectos es evidente en los derechos humanos sobre las libertades individuales de privacidad. Por otro lado, la seguridad estatal depende de las contrataciones del estado con las empresas privadas para crear lineamientos de políticas sobre seguridad nacional mostrando una relación con el crecimiento del presupuesto para seguridad y telecomunicaciones desde el 2008.

Palabras clave:

Dilema
Seguridad
Soberanía
Individual
Nacional
Telecomunicación
Tecnología
Privacidad

ABSTRACT

Sovereignty is a configured principle of multidimensional applications that include the state and individuals who are in turn affected by the dilemma that arises through its conceptualization. Recently, Ecuador has hired private telecommunications companies for the creation of a nation-wide database. The control of this database will generate a national security threat, instead of protecting it. This leads to a conceptual dilemma of sovereignty about security issues. Therefore, it is necessary to identify through the quantification of technology (e.g. number of satellites, cyber programs and telephone structures in the country), the effects that it implies. One effect is evident regarding the human right of individual freedom. Another is that state security depends on the hiring of the state with private enterprises to create policy guidelines about national security proving a correlation on the budget's increase for security and telecommunications since 2008.

Key words:

Dilemma
Security
Sovereignty
Individual
National
Telecommunication
Technology
Privacy

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

LOS EFECTOS DEL DILEMA EN LA SOBERANÍA DEL ECUADOR DE TEMAS DE SEGURIDAD NACIONAL E INDIVIDUAL DE MEDIOS INFORMÁTICOS

INTRODUCCIÓN

El Ecuador es un país democrático, soberano e independiente y pretende seguir siéndolo mediante políticas de seguridad nacional y de convenios internacionales necesarios para mantener el equilibrio de la paz. Por lo tanto, entre las principales responsabilidades del país con los individuos pertenecientes a su jurisdicción y territorio, está la de cumplir y hacer cumplir medidas de seguridad y viceversa. Sin embargo, es notable un dilema al ejecutarse políticas de seguridad en estos tiempos: La seguridad del Estado no necesariamente representa la seguridad del individuo.

La "Soberanía Estatal" y la "Soberanía Individual" entendidas por mucho tiempo como entidades conjuntas, ahora son entendidas como dos esferas distintas y separadas al presentarse temáticas de seguridad (López 2010). Esta nueva conceptualización de soberanía está vinculada con el debate actual entre privacidad personal versus seguridad nacional. Las políticas de Seguridad Nacional afectarían ambas esferas, en las libertades individuales de derechos humanos así como en nuevos riesgos y amenazas a la entidad Estatal por medio de redes tecnológicas de información.

Empero, dilemas en temáticas de seguridad no son algo nuevo. La teoría del dilema de seguridad surgió por primera vez en 1951 por John H. Herz cuando publicó el '*Realismo Político e Idealismo Político*'. En este libro, él describía el dilema de seguridad como la "autoprotección de los estados para cuidar de sus necesidades de seguridad". Esta autoprotección se daba en términos defensivos y preventivos traducidos en capacidades de

‘*hard power’* o, capacidades militares que eran vistas por los países vecinos como posibles amenazas a su integridad. Entonces, era difícil distinguir entre políticas defensivas u ofensivas, la mejor solución para los otros actores era defenderse con capacidades militares que daban la percepción al primer Estado de posibles amenazas desembocando en un modelo espiral de seguridad. Es decir, entre más inseguridades, más insegura se volvía la región por la desconfianza en los intereses del otro actor, resultando en carreras armamentísticas por las conductas ofensiva y defensiva distinguible o no distinguible (Jervis 1978).

Con la revolución tecnológica actual, la recolección de información llegó a tomar un lugar preferente en relación a seguridad, incluso desplazando a algunas capacidades militares tradicionales frecuentemente utilizadas en guerras pasadas. Esto no quiere decir que no se usaba tecnología para recolección de datos en épocas anteriores, pues la tecnología disponible en cada época permitía a las instituciones de inteligencia militar, considerada como la captación y recolección de información sobre las capacidades e intenciones del enemigo, lograr objetivos militares puntuales con poco personal y menos costos de desplazamiento. Las redes de información aún son una ventaja para cualquier país, pues permite la comunicación constante, aunque no la vuelve más transparente.

No obstante, tras los atentados del 9/11, el dilema tradicional tomó la forma de un debate tecnológico y de concebir al enemigo como cualquier individuo, puesto que los estados volcaron sus capacidades tecnológicas de recolección de información hacia sus propios habitantes, en la medida en la que el enemigo era poco reconocible y se movía en espacios internos diferenciándolo de la definición del enemigo de las guerras tradicionales. En esta situación de desesperación por otorgar seguridad nacional a los habitantes, se concluyó que el poseer una amplia base de datos de los individuos era positivo: entre más información, más seguridad. Sin embargo, esta afirmación no es tomada cien por ciento como verdadera.

El pensamiento que los líderes gubernamentales toman, es muy parecido al que se tenía sobre las capacidades militares en el dilema de seguridad original. La diferencia es que el 'enemigo identificado' aquí, son las propias personas a las cuales el Estado debe proteger (Asamblea Nacional 2008). De esta manera, no se puede distinguir si la información personal ni la recolección de su información son políticas defensivas u ofensivas, incluyendo las violaciones a los derechos humanos garantizados en cada Estado. Entre más seguridad nacional de medios informáticos, menos libertad individual y por lo tanto menos seguridad personal, garantizada en todos los instrumentos de Derechos Humanos. Dadas las condiciones y los términos en los que la seguridad nacional se debe definir y defender actualmente, se puede encontrar que la relación entre seguridad y privacidad es inversamente proporcional. Es decir, a más rigurosidad en términos de seguridad nacional, menos capacidad de los Estados de respetar la privacidad de sus ciudadanos.

Pero el dilema se complica aún más, en el sentido en que no es el Estado quien recolecta esta información, sino las empresas de telecomunicaciones privadas. Entre las razones se encuentran los contratos comerciales dentro del país de las empresas que proveen los servicios de red y telefonía. Algunos ejemplos son: Claro, Movistar, etc. Más adelante se mostrará el alcance del enlace entre Estado y empresas privadas de telecomunicaciones. Las secciones muestran que tales compañías se rigen bajo escasos estándares de control y que la información que manejan puede ser manipulada y vendida a terceros actores afectando también la soberanía y seguridad nacional. Cabe mencionar que aún no se conoce un caso específico (internacional o local) en el que las empresas hayan proveído de información nacional a otros países, pero no significa que no pueda pasar. De hecho, las mayores fugas de información secreta y delicada para la seguridad nacional de algunos Estados se han dado gracias a la intervención de hackers que juegan al borde de la ilegalidad.

Edward Snowden y Julian Assange (Wikileaks) son dos de los hackers más conocidos en la historia contemporánea, debido a la gran cantidad de datos y secretos de los Estados Unidos y de Europa que sacaron a la luz por medio de hackeos y extracción ilegal de datos confidenciales. Ambos son expertos en seguridad computarizada y publicaron evidencia de miles de datos y registros secretos, tales como el diseño y funcionamiento del programa estadounidense de recolección de datos 'PRISM', llevado a cabo por la National Security Agency. Esta evidencia fue recogida por el periodista Timothy Lee, en un artículo del *The Washington Post* del 12 de junio del 2013, en el cual empresas desmintieron haber participado en las comitivas de buscadores de información de la NSA, aunque habían llevado trasmitiendo secretamente información privada de sus usuarios al gobierno federal a partir del 2001 (Lee 2013).

Este no fue un caso aislado, muchos países reportaron ejercer algún mecanismo de obtención de información para motivos de seguridad nacional por medio de agencias telefónicas y otros mecanismos de captación de datos personales de sus ciudadanos. Como dijo Pérez (2006),

> La erosión de la soberanía de los Estados en la era de la globalización ha contribuido a la defensa de la universalidad de los derechos humanos, que ha sufrido fracasos y se ha visto en muchas ocasiones limitada por el ejercicio de la soberanía estatal.

Esto, provocó una conmoción en el mundo entero llevando a la palestra, el debate entre privacidad y seguridad. En sí, la globalización trajo consigo un nuevo dilema de soberanía y seguridad.

Teniendo en cuenta que en Ecuador la soberanía constituye uno de los más importantes atributos del Estado: podemos encontrar entre sus funciones una implicación de protección a la seguridad y vida de los ciudadanos. La intervención del tópico de "Seguridad"

permite la presencia de un discurso internacional, donde surge la pregunta: ¿Es la Seguridad Individual un límite a la Soberanía Estatal? (Deng 1995). Viéndolo desde un enfoque de derechos humanos, la respuesta es Sí, debido a que los intereses nacionales deben estar fijados con los parámetros de la comunidad internacional y la sociedad civil (Larrea 2008a, 23). Empero, desde la concepción nacional, la seguridad individual No representa una limitación (Larrea 2008b, 96). En este caso en particular, los medios informáticos son una limitación para la seguridad nacional.

Es imposible imaginar actualmente que el concepto de seguridad no involucre a las personas y solo a los Estados. “Las cuestiones relativas a la soberanía y la intervención no afectan únicamente a los derechos o prerrogativas de los Estados, sino que tienen una profunda y fundamental repercusión en cada ser humano” (López 2010, 187). Pero, el beneficiar únicamente al individuo es un menosprecio a la seguridad colectiva. Entonces, no se cumple una de las concepciones más antiguas del Estado como la que presentó Jean-Jacques Rousseau en la que el Estado cumple esta función de entidad política sobreprotectora de la población por medio de un contrato social en el que los individuos mismos ceden derechos y adquieren deberes (Rousseau 1910). Es importante reconocer que aquí el Estado toma la forma de agente protector del individuo.

Con los roles definidos entre Estado e individuos y sus relaciones ambiguas, el dilema toma forma de algunas variables. Siendo Soberanía (X) y Libertad (Y) las variables independientes; y Seguridad (Z) la variable dependiente y considerando que el objetivo fundamental es alcanzar la máxima seguridad, el dilema se refleja así:

1. Estado: Entre más soberanía estatal, menos libertad individual, igual más seguridad nacional. Sin embargo, hay una fuerte evidencia que muestra un resultado negativo en la seguridad nacional.

2. Individuo: Entre más soberanía individual, más libertad individual, igual menos seguridad nacional.

Tabla 1:[1]

	Soberanía estatal	**Libertad individual**	**Seguridad nacional**
	X	**Y**	**Z**
Estado	+	-	+ -
Individuo	-	+	-

El dilema es evidente en la Tabla 1 y el mejor resultado para propósitos de seguridad nacional también es evidente. Como se explicó anteriormente, el tener que confiar de empresas multinacionales no originarias de nuestro país como proveedoras de seguridad pone en riesgo la seguridad en una mayor escala. Incluso, la información no proporciona confiabilidad y es fácilmente transferible a otros actores. Por lo tanto, la seguridad nacional tiene como resultados: positivo o negativo. Este trabajo de investigación pretende averiguar cuál tiene más peso. Si llegara a ser positivo el aseguramiento en ambas partes con las políticas que se plantean por medio de las empresas entonces se logra la meta deseada de obtener el bien común de todos. De ser negativo el resultado de las políticas y riesgos que se contraen, sería preferible elegir un no control por parte del Estado y una preferencia para las libertades individuales defendidas.

[1] La tabla fue realizada por el autor.

Por otro lado, si solo se considera la parte individual, esta también afectaría o incluso llegaría a amenazar al Estado. A pesar de todo esto, la Soberanía Estatal ganaría más peso en el debate sobre seguridad. Las distribuciones del tema sobre el dilema en este trabajo serán las siguientes. La sección 1 definirá la primera parte del dilema concerniente a 'Soberanía'. Una clara distinción entre las dos partes mencionadas permitirá aclarar la problemática que existe dentro de las variables independientes y sus consecuencias en las atribuciones estatales y las libertades individuales en materia constitucional y de derechos humanos. La sección 2 definirá 'Seguridad' y la medición para este estudio en las políticas de seguridad con sus respectivas ventajas y desventajas. Así también, se mostrará una proyección del gasto en seguridad nacional desde el 2008.

DESARROLLO DEL TEMA

SECCIÓN 1

CONCEPTUALIZACIÓN DE SOBERANÍA PARA TEMÁTICAS DE SEGURIDAD

PRINCIPIOS DE SOBERANÍA

El siglo XXI requiere un planteamiento de Soberanía donde se tomen en cuenta las concepciones tradicionales y un enfoque especial en seguridad, donde la democracia participativa abarque nuevas estrategias, lineamientos y participación ciudadana. Es así que, dentro del marco teórico con el propósito de encontrar la definición exacta de soberanía han surgido algunas opciones, sin embargo ningún concepto ha sido universalizado. Ahora bien, tomando en cuenta la definición clásica de "soberanía" en general, ésta es la aceptación interna de cómo se organiza el estado en su estructura y formación[2]. En contraste con la concepción histórica, donde se empieza por la necesidad externa de otros países hacia el estado haciendo referencia en "la capacidad que tiene un estado nacional de ser reconocido como tal por los otros estados" y la de soberanía interdependiente que: "se relaciona con mecanismos cooperativos entre Estados y permite regular y complementar desde flujo de información, bienes, capitales, etc., que fomenten mecanismos de integración" (Larrea 2008b, 98-99). Estas interacciones son necesarias para la existencia y aprendizaje de soberanía entre naciones.

La integración por medio de las relaciones internacionales permite el flujo de información entre estado-estado y estado-individuo. Eugenia López (2010) describe a la

[2] La concepción clásica de soberanía nace en 1648 con el nacimiento del Estado-nación con la paz de Westfalia en la que cada Estado tiene la capacidad de gobernarse sin la intervención de otros estados.

soberanía como un atributo importante de los estados con la responsabilidad sujeta de velar por los intereses nacionales soberanos, se expresa así:

> Supone el reconocimiento mutuo de los Estados de su igual valía y dignidad y es condición necesaria y básica para la protección de la identidad singular y la libertad nacional y del derecho de configurar y determinar su propio destino (186).

Sin embargo, cada estado debe poseer también "la capacidad de garantizar la integridad territorial, integridad y dignidad de sus ciudadanos y de la población en su conjunto" de velar que toda información sea respetada y libre (Larrea 2008b, 100). En este contexto, los países desarrollan sus propias temáticas de soberanía por medio de procesos históricos en los cuales soberanía se ha originado, desarrollado y defendido en un enfoque individual y estatal.

Además de estos conceptos, para propósitos de este trabajo, se tomará la definición de Popovski (2009) sobre la separación de 'Soberanía' en dos esferas. La primera esfera, Soberanía Estatal en el sentido más básico de aceptación exterior en el que los Estados no son más entendidos como los instrumentos al servicio de la gente. La segunda esfera, la Soberanía Individual entendida como la libertad fundamental de cada individuo basado en la Carta de las Naciones Unidas, La Declaración Universal de Derechos Humanos y los Tratados Internacionales. Incluso, la soberanía como responsabilidad se enfoca en las responsabilidades del gobierno a favor de la población en otorgarle tales principios. Dentro de todas estas libertades, esta sección pretende enfocarse en la libertad específica de la Red, clase de libertad contemplada en los derechos de tercera generación[3] también embarcados en los derechos humanos explicados más adelante.

[3] La libertad de red contemplada en los derechos de tercera generación en derechos humanos. "No obstante, la clasificación de los derechos humanos en generaciones, más allá de la coincidencia general sobre las dos primeras generaciones (civiles y políticos; económicos, sociales y culturales), no siempre es coincidente por parte de los distintos autores, incluyendo en ocasiones una cuarta generación o tratando los derechos de determinados colectivos, como

La responsabilidad mencionada en el párrafo anterior con respecto a libertad de Red está también incluida en la concepción libertaria heredada de la Modernidad: supone una concepción de libertad más atractiva, sin limitaciones de las dimensiones por las cuales el individuo se pueda expresar (Carpintero 1989). Así fue como empezó la idea de *Freenet* (Quirós, 71-97) que cada vez está más apartada de la realidad por las barreras impuestas por las autoridades públicas (Díaz 2010, 123). Díaz (2010) indica que por el otro extremo están las entidades Estatales tratando de ser agentes fiscalizadores de la información y la Red, constatando que:

> La circulación de información tiene pues naturaleza *transfonteriza*, por tanto, un gobierno jamás podrá hacerse con el control absoluto por sí mismo; solo tiene dos alternativas, o cierra completamente el acceso a la red, o cuenta con los demás Estados y negocia con ellos un control más o menos compartido (124).

Para Moles (2004) esta idea de fiscalizar la Red es compartida por gobiernos totalitarios y democráticos. Por ello, es vital el análisis del binomio soberanía-libertad que él propone, sea más específico para la defensa de las libertades de redes de comunicación de la ciudadanía:

> Internet, comienza a ser un reto para los gobiernos que buscan, alegando razones de interés general y de seguridad pública, una justificación o legitimidad para controlar la localización y el acceso de información en la red, así como una necesidad de identificar a los usuarios que envían determinados mensajes o acceden a un sitio de Internet concreto (22).

Con la violación a estas defensas de libertad es evidente una fisura también en la concepción de Soberanía como explica Popovski (2009). Como expresa la idea de *Freenet* para el acceso libre del Internet, las barreras entre ambas esferas están muy separadas y necesitan de una conceptualización clara para proporcionar un entendimiento de las diferencias entre ambas esferas: estatal e individual.

---

las mujeres, los menores, los refugiados, o los homosexuales, dentro de una generación especial" (Amnistía Internacional, s.f.). Extraído el 6 de Mayo de 2016. http://www.amnistiacatalunya.org/edu/es/historia/dh-futuros.html

ESFERA ESTATAL E INDIVIDUAL

Generalmente, el concepto de ‘Soberanía’ embarcaría una conceptualización amplia y general de todo lo intrínseco de la jurisdicción nacional. En este caso, la Soberanía Estatal es la representación de todo el cuerpo institucional, ejecutivo, legislativo, judicial, administrativo, etc. que pertenece a la maquinaria Estatal y a sus intereses. A su vez tiene el deber de representar al país y defenderlo de amenazas externas e internas, considerando que los intereses que priman son los de la Nación como ente general. La esfera Estatal no sitúa al individuo como agente de creación, acción y ejecución de políticas públicas, sino como agente sobre el que se aplican tales políticas (Larrea 2008a, 13).

En contraste, la Soberanía Individual es la soberanía en su concepto más idealista y libertario, en la que el Estado sirve al individuo y, las políticas no actúan sobre el individuo. Al contrario, el individuo actúa sobre ellas. Estas políticas, defienden y proveen los avales necesarios para que se respeten las libertades garantizadas de convivencia ubicando al Estado como ente protector del individuo al cual se debe servir y no restringir. Esta libertad que reclama la esfera individual es la que entra en conflicto directo con la esfera estatal. Pues la esfera estatal trata de enmarcar, limitar territorio y libertades para garantizar la libertad colectiva. De ahí proviene la creación de leyes para limitar el comportamiento del individuo. Libertades de la esfera individual como la de información entra en conflicto directo con las prerrogativas de un Estado que busca garantizar la libertad colectiva. Conflicto que se da cuando existen dos ideas contrapuestas que son de origen político e irreconciliables a través del tiempo al punto de afectar los derechos civiles y humanos de las personas (Fraga 1962, 3).

En el Ecuador, ambos enfoques son contrapuestos; ambos se expresan sobre el Estado al referirse a temáticas de Seguridad. De un lado el Estado como unidad política tiene el deber

de “proveer y garantizar normativamente la seguridad tanto de las amenazas de ataque de Estados enemigos (seguridad externa) como del orden público y la convivencia pacífica de sus habitantes en un determinado territorio (seguridad interna)” (Larrea 2008b, 39). Del otro lado, difieren desde una concepción internacional en el que se violarían derechos inmiscuidos en el individuo como la libertad personal. A continuación se detallarán algunos principios de la legalidad de las libertades existentes en el Ecuador en el binomio soberanía-libertad.

Principios fundamentales de libertad y derechos humanos

En materia de Derechos Humanos el ser humano es el sujeto de derechos al cual el Estado debe proteger y garantizar el goce más amplio de sus libertades. Este principio es clave a la hora de definir políticas de seguridad que no atenten contra la soberanía. En este sentido, el Ecuador también:

> Considera al ser humano como el objetivo sobre el cual se ha de edificar toda política encaminada a buscar el desarrollo social, económico y político de la nación, y como el punto de referencia para la política exterior del país. Para que el individuo pueda desarrollarse en libertad y con dignidad, potenciando todas sus capacidades, es fundamental que el Estado le asegure el goce y la defensa de sus Derechos Humanos. El Ecuador respalda y propugna la indivisibilidad, interdependencia, universalidad e integralidad de los mismos, lo que significa que otorga igual relevancia a los derechos civiles y político, a los económicos, sociales y culturales, así como también, a los individuales y colectivos, y a los de tercera generación (Larrea 2008a, 13).

Los derechos de tercera generación están conformados especialmente por la erosión de la soberanía “en la era de la globalización *que* ha contribuido a la defensa de la universalidad de los derechos humanos, que ha sufrido…limitaciones por el ejercicio de la soberanía estatal” (Pérez 2006, 247). El Ecuador respalda y defiende los derechos de tercera generación, sin embargo en los últimos años ha existido una clara distinción en ambas esferas: nacional e individual.

Entre otras garantías, el Gobierno Nacional dentro de los principios fundamentales en la Constitución actual del Ecuador expresa que "la soberanía radica en el pueblo, cuya voluntad es el fundamento de la autoridad" (Asamblea Nacional Constituyente 2008). Es por eso que el Artículo (Art) 3. Numeral 2: "Garantizar y defender la soberanía nacional" está como principio fundamental de los deberes primordiales del Estado. Por otra parte, la Ley Orgánica de Comunicación del Ecuador también plantea:

> Que, en el Estado constitucional de derechos y justicia, en concordancia con principios y normas de la Convención Interamericana sobre Derechos Humanos, se reconocen los derechos a la comunicación, que comprenden: libertad de expresión, información y acceso en igualdad de condiciones al espectro radioeléctrico y las tecnologías de información y comunicación; (Asamblea Nacional 2013)

Según estos principios, es necesario preguntarse: ¿están ambas soberanías en peligro constantemente? En este siglo, las amenazas están estructuradas en forma de información digital, poniendo en riesgo a la "Seguridad, Desarrollo y Derechos de Tercera Generación: El caso de la libertad informática" según lo plantea Díaz (2010, 111).

Derecho de libertad individual y privacidad de información

La libertad individual y su privacidad son dos derechos considerados en la nueva Constitución del País (Asamblea Nacional 2008), expresados de la siguiente manera:

> Art. 16.- Todas las personas, en forma individual o colectiva, tienen derecho a: Numeral 2. El acceso universal a las tecnologías de información y comunicación.
>
> Art. 17.- Numeral 2.- Facilitar la creación y el fortalecimiento de medios de comunicación públicos, privados y comunitarios, así como el acceso universal a las tecnologías de información y comunicación… (16) y

La **Ley Orgánica de Comunicación (LOC)** define libertad de información de la siguiente manera:

> Art. 29.- Libertad de información.- Todas las personas tienen derecho a recibir, buscar, producir y difundir información por cualquier medio o canal y a seleccionar libremente los medios o canales por los que acceden a información y contenidos de cualquier tipo.
>
> Esta libertad solo puede limitarse fundadamente mediante el establecimiento previo y explícito de causas contempladas en la ley, la Constitución o un instrumento internacional de derechos humanos, y solo en la medida que esto sea indispensable para el ejercicio de otros derechos fundamentales o el mantenimiento del orden constituido…(Asamblea Nacional 2013, 7)

Teniendo en cuenta que la libertad de información está condicionada al mantenimiento del orden establecido para no respetar el derecho mencionado, sobre la privacidad de información la LOC estipula:

> Art. 31.- Derecho a la protección de las comunicaciones personales.- Todas las personas tienen derecho a la inviolabilidad y al secreto de sus comunicaciones personales, ya sea que éstas se hayan realizado verbalmente, a través de las redes y servicios de telecomunicaciones legalmente autorizadas o estén soportadas en papel o dispositivos de almacenamiento electrónico.
>
> Queda prohibido grabar o registrar por cualquier medio las comunicaciones personales de terceros sin que ellos hayan conocido y autorizado dicha grabación o registro, salvo el caso de las investigaciones encubiertas autorizadas y ordenadas por un juez competente y ejecutadas de acuerdo a la ley.
>
> La violación de este derecho será sancionado de acuerdo a la ley (Asamblea Nacional 2013, 7) .

Los artículos mencionados hacen énfasis en que toda persona debe gozar de la libertad de acceso a tecnologías de información. Empero, ¿es esta información libre? Mediante la facilitación de la creación y fortalecimiento de nuevos medios de comunicación públicos y privados, se restringe la libertad de comunicación. Esto indica la necesidad de un órgano de control, ya sea público o privado. Así lo estipula el párrafo dos del Art. 29 de la LOC en el que la circulación libre de información puede limitarse solo por causas contempladas en la ley.

Entre las razones para limitar el libre acceso de información están la prevención de amenazas contra la soberanía, pues tales amenazas impedirían el ejercicio de los derechos hacia otros ciudadanos y al Estado. En lo que respecta a privacidad de información estas

tienen derecho de inviolabilidad. El único autorizado para hacer grabaciones o recepciones de información es el Estado por propósitos establecidos en la ley. En consecuencia, se hace énfasis en que una de las principales funciones del Estado es "Garantizar y defender la soberanía nacional" (Asamblea Nacional 2008) respetando los derechos humanos, así como las libertades de información. Sin embargo estos derechos están bajo la interpretación del gobierno y no son considerados universales. Es decir, en la medida que un individuo represente una amenaza, no son tomados en consideración. A continuación, se presentan cuáles son las posibles amenazas para la soberanía, tanto estatal como individual.

AMENAZAS A LA SOBERANÍA ESTATAL E INDIVIDUAL

Con la modernización de los Estados y las comunidades, una amenaza emergente es el riesgo de la información proporcionada por los usuarios a las empresas de telefonía local e internacional sin el debido consentimiento o permiso. La **información digital sensible** es el registro de llamadas recibidas y enviadas, así como el de mensajes entrantes y salientes por medio de cualquier dispositivo fijo y portátil, chats y videos ([IS] 2016). Es una ventaja y desventaja de tercera generación (Díaz 2010, 118). Díaz (2010) también expone que en estas posibilidades de desarrollo se destacan algunos riesgos:

a) "riesgos derivados de una posible hiperinformación (que nos impide distinguir entre lo importante y lo secundario), o de la ausencia de calidad o veracidad de lo que se pone a disposición de la sociedad, o de la ilicitud de los contenidos (que pueden ser racistas, violentos, difamatorios, ofensivos, etc.);
b) riesgos derivados de la brecha digital, que daría lugar a una discriminación mayor con respecto a los sectores sociales más desfavorecidos, cuya ausencia de la red limitaría sus oportunidades de desarrollo (encontrar un trabajo, una información, un artículo de compra a mejor precio, etc.)frente a los que tienen acceso;
c) riesgos para la privacidad de la persona y, por lo tanto, para el desarrollo personal por injerencias ajenas en los campos íntimos del usuario (seguridad en la navegación y de las bases de datos);
d) riesgos para el desarrollo personal por abuso o falta de moderación y responsabilidad en el uso de Internet (adicción) o por el aislamiento que pueda suponer frente al entorno familiar y social (deshumanización del individuo);

e) riesgos para los sectores sociales más débiles, como pueden ser los menores (pornografía infantil, proposiciones de pedofilia, etc.);
f) riesgos en las transacciones comerciales y bancarias;
g) riesgos para la integridad de los instrumentos informáticos (virus, apropiación *online* del equipo, etc.);
h) riesgos en el campo de la propiedad intelectual e industrial;[4]
i) riesgos de quiebra de principios judiciales, que pueden impedir o dificultar la aplicación del derecho a ciudadanos extranjeros;
j) riesgos para la seguridad nacional, como denunció la India con respecto al servicio de Google Earth" (120-121).

Estas amenazas son consideradas de tercera generación porque generan una amenaza no existente antes del Internet. Entre los riesgos que menciona Díaz es importante recalcar la intervención de las empresas de telefonía y comunicaciones como proveedoras del servicio de Red. Estas amenazas funcionan en ambos lados, pero los únicos que pueden ejercer políticas generales en contra de estas es el gobierno. El individuo también se ve afectado según los artículos mencionados. En resumen, los riesgos más relevantes para el tema de esta investigación son literales a), c), d) y h), especialmente: **c)** y **h)** muestran evidencia para el dilema en la privacidad de las personas en base de datos y los riesgos para la seguridad nacional.

Durante toda esta sección, se presentó las correctas conceptualizaciones de soberanía para que el lector tenga un enfoque general y tome parte considerando el dilema intrínseco que existe en el país. Las prerrogativas estatales y las libertades individuales se presentaron de la misma manera para evidenciar los posibles riesgos del dilema mencionado: riesgos a nivel nacional así como de las violaciones a los derechos humanos y constitucionales de nuestro país. Empero, estos mismos derechos también influyen en la Seguridad Nacional. En la siguiente sección, se especificará en materia de Seguridad Nacional e Individual los literales mencionados. Las limitaciones y ventajas al contratar empresas tecnológicas extranjeras por

[4] Negrilla añadida por el autor.

razones tecnológicas y de alcance y sus consecuencias directas en la percepción de seguridad individual.

SECCIÓN 2

CONCEPTUALIZACIÓN DE SEGURIDAD

Para un correcto enfoque de Seguridad es importarte analizar las dinámicas de seguridad entre los Estados. Es notable que los tomadores de decisiones sean los individuos, quienes conforman a los Estados del mundo. Por consiguiente, son los deseos humanos los que reflejan las políticas exteriores de los Estados (Morgenthau 1986). Entonces, el término "seguridad" debe considerar todos los aspectos relevantes desde el ámbito internacional hasta el individual. Siendo Ecuador parte de esta sociedad internacional, es relevante partir desde una perspectiva externa para poder entender internamente la problemática.

SEGURIDAD EN EL ÁMBITO INTERNACIONAL

Partiendo de la conceptualización universal de la ONU, la seguridad humana nace del marco normativo dinámico y práctico. Entonces, los gobiernos son los responsables directos de ejecutar los planes necesarios para que se respeten la seguridad y soberanía personal. "De la misma manera, las organizaciones regionales y subregionales desempeñan un papel fundamental en la movilización del apoyo y la promoción de la actuación colectiva" (United Nations Trust Fund for Human Security 2016). Es de suma importancia analizar los planteamientos que esta conceptualización ha generado y una especial atención a "las amenazas existentes y emergentes para la seguridad y el bienestar de las personas y las comunidades" (United Nations Trust Fund for Human Security 2016). El concepto de seguridad estipulado por la ONU coloca en primer lugar a la dignidad humana y el necesario replanteamiento del mismo cuando este representa un fundamento primordial para la Seguridad Nacional.

En el plano regional, la Declaración sobre la Seguridad en las Américas reafirma "que la seguridad en el Hemisferio tiene como base fundamental el respeto a los principios consagrados en la Carta de las Naciones Unidas y en la Carta de la Organización de los Estados Americanos" (Organización de los Estados Americanos, 2003). Entre ellos, el respeto a las libertades individuales y al Estado de Derecho estipulado en ambas Cartas son de igual importancia como bases de toda Declaración, estrategia o plan de acción Estatal o Convención. La misma declaración provee un enfoque multidimensional para los Estados en cultura de seguridad cibernética, como lo estipula el Art. 26:

> Desarrollaremos una cultura de seguridad cibernética en las Américas adoptando medidas de prevención eficaces para prever, tratar y responder a los ataques cibernéticos, cualquiera sea su origen, luchando contra las amenazas cibernéticas y la delincuencia cibernética, tipificando los ataques contra el espacio cibernético, protegiendo la infraestructura crítica y asegurando las redes de los sistemas(…)teniendo en cuenta el trabajo que desarrollan los Estados Miembros coordinado con la Comisión de Seguridad Hemisférica (2003 9-10).

Creando una cultura de seguridad cibernética, se delimitará las acciones de los países involucrados y sus habitantes, sobre todo cuando la seguridad está altamente relacionada con la soberanía. Localmente, el gobierno ecuatoriano está planteando nuevas estrategias y lineamientos que involucren al ciudadano de manera más integral. El propósito es poder categorizar las ventajas de un sistema seguro de información que no atente la soberanía estatal. En este proceso, también se intenta identificar posibles amenazas cibernéticas y una mejora en la infraestructura tecnológica, desembocando en un aumento al presupuesto en Seguridad Nacional.

SEGURIDAD CIBERNÉTICA ESTATAL

En el Ecuador, la nueva Política de Seguridad establece la priorización de las estrategias y acciones a favor de defender la integridad soberana e independiente de la ciudadanía en sus ámbitos político, cultural, económico y de desarrollo social (Larrea 2008b,

98). Considerando el Plan Estratégico de Seguridad Nacional, lineamiento estratégico 4.4.4 se debe promover en el marco regional y subregional el combate de las amenazas al espacio cibernético. El lineamiento estipula:

> 4.4.1. Desarrollar una cultura de seguridad cibernética en el país y fomentar tal cultura a nivel regional y subregional; adoptar medidas de prevención eficaces para evitar, tratar y responder a los ataques cibernéticos, cualesquiera sean sus orígenes, para luchar, así, contra las amenazas y la delincuencia cibernética, y, a su vez, tipificar, adecuadamente, los ataques contra dicho espacio (Larrea 2008a, 49).

Los orígenes de los ataques cibernéticos pueden ser internos. De tal manera se debe priorizar la Seguridad Estatal sobre la Seguridad Individual en todo aspecto vulnerable. El Estado debe asegurar su bienestar para poder asegurar y tomar las mejores decisiones para la seguridad del bienestar colectivo, incluso al riesgo de afectar en cierta proporción la Seguridad Individual. Sin embargo, Ecuador no cuenta con la tecnificación necesaria para defenderse en contra de un ataque cibernético interno (considerado como el acceso a información sensible presentada por el individuo o institución) que llegue a generar una crisis mayor a la nación, región o mundo, ni para prevenirla por medio de la invasión a la privacidad (Instituto Ecuatoriano de Propiedad Intelectual 2015). La situación de sensibilidad se da porque la información no es tangible. Al contrario es muy rápida y dispersa, capaz de viajar en segundos al otro lado del mundo por medio de la red. Además, hasta el 7 de Junio, 2013, el Sitio Web Información Sensible[5] actualizó el concepto de **'información sensible'** como la información legal de miles de correos, conversaciones de chat, imágenes o vídeos ([IS] 2013).

Un claro ejemplo el uso de los contratos secretos que las agencias de inteligencia norteamericana tenían en su momento con las empresas telefónicas para acceder a toda información sensible era justificado para la intromisión a la soberanía individual para

[5] [IS] Información sensible. Último acceso el 2 de febrero de 2016. http://www.informacionsensible.com/

propósitos de seguridad (Morales 2004). Ecuador ha intentado copiar los mecanismos que usaban las agencias de inteligencia extranjeras cuya responsabilidad era manejar toda información legal sensible. Estos procesos resultan muy costosos, delicados y subjetivos. Hasta ahora se ha propuesto que las empresas telefónicas extranjeras tomen el control para proveer dicha información al Estado cuando sea requerida.[6] Sin embargo, se reconoce que

> Con el propósito de alcanzar la soberanía y autonomía tecnológica que derive en ahorro de recursos públicos (…) actualmente las entidades públicas tienen en sus planificaciones o se encuentran en ejecución de este traspaso, por lo que los nuevos proyectos informáticos están considerando la adopción de herramientas de Software Libre[7] que forjará en el país innovadores independientes de la tecnología extranjera (Instituto Ecuatoriano de Propiedad Intelectual 2015).

Pero hasta que el Estado se modernice, toda información sensible correspondiente a miles de datos informáticos debe pasar por filtros tecnológicos para dar resultados eficientes sobre; es decir, lo que representa una amenaza o no. El país no puede esperar modernizar sus sistemas informáticos, por lo tanto debe depender de asignaciones o dependencias tecnológicas.

Limitaciones del Estado

Para que el Estado posea tal información, se delegan asignaciones mediante contratos comerciales para operar en el país a empresas multinacionales que muestra limitaciones del poder estatal. A continuación, se presentarán cinco limitaciones del Estado como agente de control. **Primero, el poder de negociación que se produce por la necesidad del servicio:** Esto ha otorgado una ventaja de negociación a las empresas de telecomunicación cuando contraen un convenio/contrato comercial de operación en el territorio. Entre estas ventajas de

[6] Este supuesto está fundado en los antecedentes presentados en la introducción con el escándalo de PRISM en EE.UU.

[7] "El Software Libre permite establecer infraestructuras propias y descentralizadas que optimizan los recursos y fortalece el talento humano, incentivándolo a la innovación" http://www.propiedadintelectual.gob.ec/software-libre-politica-publica-y-alternativa-para-defenderse-del-espionaje-cibernertico/

negociación constan las garantías en los contratos de ganancias económicas al Estado por medio de impuestos y otros beneficios. Las transnacionales se comprometen a dar información privada individual cuando el Estado lo requiera por temas de seguridad nacional, en el que ambas partes resultan favorecidas (Asamblea Nacional 2013).

Segundo, la falta de autentificación de datos: Es evidente como las redes de comunicación han sido dominadas por empresas privadas que a su vez disponen de grandes cantidades de información. Estas obtienen voluminosas bases de datos voluntariamente por parte de los usuarios mediante el proceso de aceptación de términos en los requisitos llenados y acuerdos de uso que el usuario por lo general no lee. Por otra parte *Firefox*, un buscador popular de internet, invita a los usuarios a leer los términos de privacidad y ofrece a los navegantes de la red una línea de seguridad en contra del espionaje para que se pueda navegar por el internet con tranquilidad (Dixon, 2015). Algunas empresas se han unido a esta iniciativa, como *Apple* y *Whatsapp* para distinguirse del resto en vender privacidad individual. La limitación de autenticidad de datos indica que se deberá separar, clasificar y categorizar información en cuestión de minutos. En este caso, las empresas poseen buscadores especializados para detectar anomalías o categorizar a los individuos por búsquedas en internet.

Tercero, las desventajas tecnológicas del país se pueden dividir en algunas subsecciones, pero cabe mencionar las tres que se podrían considerar las más importantes.

1) El número de satélites que las empresas poseen en la región y que el Estado no posee son claves porque permiten el viaje de información de una manera rápida y eficaz. Además de una posición estratégica en la órbita espacial que permite “una cobertura mucho

mayor que un enlace inalámbrico fijo o móvil, no obstante utiliza una infraestructura de red mucho más compleja por lo que sus costos son mucho mayores" (ARCOTEL 2015b).

En la región, el Congreso Latinoamericano de Comunicaciones Satelitales y Radiofusión (LATSAT), reportó que en el 2013 América Latina poseía 72 satélites y se esperaría que para el 2017 el número total llegue a 26 más (El País 2013). De esta cantidad de satélites en Latinoamérica, el Ecuador solo representa el 2.78 % en comparación con otros países. La siguiente tabla muestra el nombre, fecha de lanzamiento y utilidad de los satélites de comunicación existentes en el espacio de origen ecuatoriano:

Tabla 2:

Satélites	**País**	**F. de lanzamiento**	**Utilidad**
Pegaso	Ecuador	25-Ene-13	Vista de la tierra en el espacio en tiempo real.
Krysaor	Ecuador	21-Nov-13	Actúa como radar para identificar cualquier objeto que orbite cerca del espacio y de la tierra.

Información extraída de EXA[8]

Es importante distinguir entre estos dos satélites y los comerciales que operan y orbitan la zona ecuatoriana y la región, los cuales son muchos más. JJ Velasco en el blog oficial de *Telefonica* el 23 de Julio del 2013 publicó que desde 1962 se mandan satélites comerciales de comunicaciones al espacio. El primero fue el histórico Telstar 1(Estados Unidos), en un tiempo en que todo uso era militar. Con ese proyecto, la NASA y la American Telephone and Telegraph Corporation (AT&T) se unieron para "desarrollar un sistema de comunicaciones por satélite comercial para su uso en la difusión de señales de radio y televisión así como en telefonía fija" (Velasco 2013). En lo que respecta a esta época, un artículo del *New York Times* menciona que la empresa AT&T ayudó a la Agencia de Seguridad Nacional a recopilar billones de correos electrónicos en un periodo que según la

[8] Agencia Espacial Civil Ecuatoriana, EXA, Revisado el 7 de Marzo de 2016. http://exa.ec/

evidencia presentada ante la ONU provenía desde el 2003 al 2013.[9] Esta es una de las razones por las que el Ecuador apuesta por la contratación de empresas privadas de telecomunicación a pesar de los elevados costos, pues le permite al Estado un control mayor de información (Angwin et al. 2015).

En el Ecuador, la Agencia de Regulación y Control de las Telecomunicaciones 'ARCOTEL' presenta los techos tarifarios de algunas empresas operadoras en servicios móviles por satélite como LEOSATELLITE S.A, COMSATEL S.A, CARSEG S.A, ABINSA, ALMEIDA BRANDS, VISTASPAC, ELECTROMARINA S.A, LINKSAT y NAUTICAL. No obstante, el usar un satélite para una cobertura mayor implica también un mayor costo (ARCOTEL 2015b). Sin embargo, las ventajas de usar este tipo de comunicación en lugar de otras es que nos proporciona un respaldo de todas las conexiones terrestres y fijas. A pesar del alto costo es una garantía importante en la búsqueda privacidad estatal en contra de terceros actores. El gobierno reconoce no contar con la capacidad de almacenamiento ni tecnificación por lo que depende de los satélites comerciales privados (Instituto Ecuatoriano de Propiedad Intelectual 2015).

2) Ecuador es un escenario favorable para muchas empresas de redes móviles. Así, lo reporta el diario *El Comercio* en una publicación en la que da a conocer que además de las tres operadoras existentes en el 2014 habían tres compañías de telecomunicaciones interesadas en invertir en el país: 'Virgin Mobile', 'Multinet' y 'Olo'. Virgin, ya cuenta con experiencia en América Latina en países como Chile, Colombia y México. Multinet opera especialmente en Asia y Rusia, y Ecuador sería el primer país de la región en la que entraría. Por otro lado, Olo es una empresa peruana nueva en el mercado que intenta

[9] Estos documentos en contra de AT&T fueron presentados por Edward Snowden y revisados por el *New York Times* y ProPublica.

internacionalizarse (*El Comercio* 2014). Ninguna de estas logró entrar al mercado ecuatoriano de telecomunicaciones, pero sí 'Tuenti' de origen español en el 2015. Actualmente en el Ecuador operan cuatro operadoras móviles: Claro (México), Movistar (España), CNT y Tuenti (*El Universo* 2015), solo CNT es nacional.[10]

Las redes de celulares fueron creadas para proveer de servicios de voz, pero "a medida que la tecnología ha evolucionado los requerimientos de los usuarios han ido cambiando y es por esto que en la actualidad las nuevas tecnologías celulares están enfocadas en el servicio de datos" (ARCOTEL 2015b). Esta es una medida tecnológica necesaria para ser adquirida por el uso colectivo de las personas y su disposición móvil. Además, por la calidad de servicio que ofrecen las operadoras móviles extranjeras en comparación con la nacional, muchos optan por tener una línea de origen extranjero, aunque esta percepción en beneficios de usuarios y servicios al consumidor está cambiando.

3) Las infraestructuras de los operadores de Móvil Avanzado solo en el 2016 muestran que Claro (CONOCEL S.A) y Movistar (OTECEL S.A) tienen un mayor número mensual de sitios (estructuras) que CNT EP (ARCOTEL 2015a).

Cuarto, el control de información: De ser muchas operadoras las que presten el servicio, la información sensible se vuelve más difícil de controlar. Las empresas telefónicas dependen del gobierno para los requisitos, localidades y publicidad para trabajar y se espera por lo tanto una exclusividad nacional de ambas partes en información. Es decir, la información sensible también es atractiva a postores internacionales, sean estos países o empresas trasnacionales. Es imposible también conocer lo que le llame la atención a otro actor, además de la confiabilidad del usuario de proveer información verídica. Siendo este el

[10] ARCOTEL. (a) Techos tarifarios. Revisado el 15 de abril de 2016. http://www.arcotel.gob.ec/servicio-movil-avanzado-sma/

caso, ¿cómo se identifica que la información no es desinformación? El riesgo es la generación de políticas públicas generadas a las expectativas de esta información no confiable.

Quinto, la intriga por catalogar temas o intereses de seguridad nacional y sus amenazas: ¿Quién decide las temáticas de seguridad nacional? Si los lineamientos de seguridad cumplen un papel multidimensional al atacar diversas amenazas desde el sector policial, militar y cibernético, etc. De igual manera ¿qué es una amenaza? El campo de observación es amplio, ¿podría ser una llamada o correo a favor del candidato opositor del gobierno actual o una queja por un mal servicio público? Entonces, la línea de identificación de amenazas a la Seguridad Nacional se vuelve muy delgada. Es por eso que se deben plantear los lineamientos de Seguridad para medir lo que se pierde en los derechos individuales y de la cantidad presupuestal que se amerite.

Lineamientos y Presupuesto General en Seguridad

La fijación de políticas públicas en materia de seguridad nacional se transforma en el direccionamiento concreto de recursos estatales a fin de conseguir objetivos específicos. En este sentido, se debe considerar una urgente revisión a los temas de seguridad nacional, control estatal de la red, la integración de un sistema integral en todos los programas institucionales y la protección a la soberanía. Actualmente, cuatro de los siete "lineamientos fundamentales para construir la institucionalidad de la Seguridad como eje rector de las políticas públicas, planes y programas de los órganos estatales" (Larrea 2008b, 99) lo estipulan de igual manera:

> Núm. 1. Revisión de la Misión y Visión institucionales
>
> Núm. 4. Administración eficiente de los presupuestos

> Núm. 5. Introducción de la seguridad integral como eje transversal en sus programas institucionales
>
> Núm. 7. Protección de la soberanía nacional e integral del Estado (Larrea 2008b, 99).

Además, para cumplir tales lineamientos del Estado, el numeral 4 debe considerar un gasto en desarrollar una cultura de seguridad cibernética, mediante el incremento del gasto en seguridad en comparación a gobiernos de años anteriores. Si se cree una concientización de seguridad y los beneficios que las operadoras ofrecen al Estado, se logrará una mayor aceptación. Carrión (2005) analizó las consecuencias de la crisis económica en el presupuesto de seguridad ecuatoriano en el período 1995-inicios del 2006:

> A pesar de ciertas caídas derivadas de la crisis económica, se observa una tendencia global al aumento de las asignaciones a seguridad, con un promedio anual de 8% de crecimiento de los recursos destinados a este tema. En cifras, el presupuesto destinado a la seguridad *subió* de 800 millones de dólares, en 1995, a cerca de 1300 millones en 2006, lo que denota un incremento de 60% acumulado en 10 años (Carrión 2005)

De esta distribución, debemos solo considerar que tal presupuesto se dividía en tres sectores: Sector Judicial, Sector Asuntos Internos y Sector Defensa. Del último, solo 632,26 millones de dólares eran destinados para defensa en la asignación inicial del 2006. El presupuesto desde el 2006 a 2009 en defensa del país en millones de dólares fue el siguiente:

Tabla 3: [11]

2006	2007	2008	2009
1,212.3*	1,504.3*	2,159.1*	2,607.9*

*en millones de dólares.

A partir del 2008, con el nuevo mandato se reformaron las Estrategias sobre Seguridad, fondos y recursos que no estipulaban antes las ventajas y desventajas de la información a través de redes telefónicas y cibernéticas provocando un cambio en el índice

[11] Tabla 3. Ver índice de tablas.

presupuestal para el 2009. El presupuesto en defensa desde el 2008 a 2015 siguiente, período de la revolución ciudadana, no contempla el gasto por personal:

Tabla 4:[12]

2010	2011	2012	2013	2014
No data	1,699.50*	174,306,553.63	1,619,101,951.18	217,628,449.42

*en millones de dólares.

En el 2011, los recursos provenientes de pre asignaciones[13] fueron la tercera fuente de ingresos juntos a los ingresos "generados en su mayor parte por el Ministerio de Telecomunicaciones y Ministerio de Defensa…presentan un nivel de 23%" (Ministerio de Finanzas 2015). El incremento del presupuesto a través de los años fluctúa por los cambios en el precio del petróleo. Actualmente el presupuesto en seguridad contempla dos Ministerios, el Ministerio de Coordinación de Seguridad está en 11, 224,153.00 y en 1,682.9925.399.82 para el Ministerio de Defensa Nacional que han permitido una reestructuración de los lineamientos mencionados y la cooperación entre el área de las telecomunicaciones y la defensa nacional por motivos de seguridad nacional (Ministerio de Finanzas 2015).

Ahora bien, la sección 2 definió 'Seguridad' como interés nacional e individual, además de las ventajas y desventajas de los lineamientos en seguridad estatal. Entre las ventajas de tales lineamientos están una mayor cobertura de protección para todas las

[12] Tabla 4. Ver índice de tablas.
[13] El art. 298 de la Constitución del Ecuador (2008) señala: "Se establecen pre asignaciones presupuestarias destinadas a los gobiernos autónomos descentralizados, al sector salud, al sector educación, a la educación superior; y a la investigación, ciencia, tecnología e innovación en los términos previstos en la ley. Las transferencias correspondientes a pre asignaciones serán predecibles y automáticas. Se prohíbe crear otras pre asignaciones presupuestarias" Léon Roldos. "¿Son pre asignaciones?, ¿o qué?" En *Diario El Comercio.* Publicado el 6 de Mayo del 2016. Último acceso el 6 de mayo de 2016. http://www.elcomercio.com/opinion/son-preasignaciones.html

instituciones gubernamentales, el ingreso de temas de seguridad informática regional e internacional a la agenda nacional reflejada en un incremento en el presupuesto nacional desde el año 2008 y la creación de nuevos organismos de control de información. Por otra parte, entre las desventajas se encuentran la dependencia de tecnología privada, las violaciones a los derechos de libertades individuales, la competencia y desconfianza a nivel regional que podrían desembocar en carreras armamentísticas o de incremento de infraestructura de redes y satélites. En resumen, según la evidencia empírica mostrada, el presupuesto general y la contratación de tecnología extranjera en telecomunicaciones sí sustenta la hipótesis del dilema actual en el Ecuador por todos los riesgos que esta implica por la inexistencia de tecnología propia. Sin embargo, los intereses gubernamentales aun priman más a la hora de la toma de decisiones en seguridad.

CONCLUSIONES

Actualmente, el debate entre Privacidad Individual y Seguridad Nacional ha generado un problema de era tecnológica en la que los Estados ven la necesidad de modernizar y tecnificar. Según las conceptualizaciones mencionadas, el Estado debe proteger y supervisar la seguridad individual en ambas esferas de soberanía: la esfera individual entendida como las libertades individuales de información y derechos de tercera generación y la esfera estatal como la defensa de los intereses del Estado ante amenazas internas y externas.

Por lo tanto, la seguridad nacional procura embarcar lineamientos antes no contemplados como la tecnificación de las telecomunicaciones. Esto se fundamenta en el aumento del gasto gubernamental en seguridad. No obstante, esto representa un dilema de seguridad: la presentación de dos problemas distintos cuyas soluciones están relacionadas, una depende de la otra para sobrevivir en el cumplimiento por alcanzar el mayor bien posible. A la vez, estos problemas no pueden presentarse por separado en temas de seguridad; la una depende de la otra. Siendo el caso del gobierno destinando presupuesto estatal para contratar a empresas extranjeras de red como en el caso de EE.UU cae en el dilema y desventaja de que las compañías telefónicas manipulen y provean de la misma información a otros actores o países.

Entre las amenazas que el Estado incurre están: poner en peligro la integridad e información personal de las cuales se recopiló información. Esto viola las garantías constitucionales y de derechos humanos en libertad. Pero, por otra parte, si el Estado no se asegura localmente contratando a empresas de telecomunicaciones, no poseerá ningún tipo de control estatal y así no podrá cumplir con su rol de entidad sobreprotectora. Por esta razón, no se puede fácilmente justificar los contratos de recolección de datos por motivos de seguridad

nacional. Este control puede ser visto como obtención de un poder, que sería un arma de doble filo. Además, el país no tiene la tecnificación suficiente para ser independiente tecnológicamente, así que deberá seguir confiando ciegamente en las empresas que poseen la capacidad tecnológica en redes satelitales, redes móviles y de infraestructura.

A pesar de todo, cualquier medida que el Estado tome en proteger una o ambas esferas, producirá efectos positivos y negativos en la seguridad colectiva, que no son comparados ni significativos si solo se enfocara en la esfera individual. Como fue planteado al principio de este trabajo, un enfoque en la esfera estatal también enmarca a la esfera individual aunque en menor proporción. En conclusión, el Ecuador deberá seguir tomando políticas de seguridad como lo ha hecho, pero debería contemplar una mayor participación ciudadana y más transparencia en el uso de redes de comunicación. Se recomienda que esta base de datos no deba ser obtenida sin el consentimiento de las personas ni ilegítimamente. La información no debe ser analizada solo por medios gubernamentales, pero por comitivas civiles de ecuatorianos. La mejor manera de que una política sea aceptada por la población es con la participación constante de la misma.

REFERENCIAS BIBLIOGRÁFICAS

[IS] Información Sensible. *Estados Unidos espía a usuarios de Google, Facebook o Apple*. Última modificación el 7 de Junio, 2013, Último acceso el 2 de Febrero de 2016. http://crowdfunding.informacionsensible.com/news/483/contacto.php

Amnistía Internacional. "Los derechos de tercera generación" En Declaración Universal de los Derechos Humanos. Extraído el 6 de Mayo de 2016. http://www.amnistiacatalunya.org/edu/es/historia/dh-futuros.html

Agencia Espacial Civil Ecuatoriana, EXA, Último acceso el 7 de Marzo de 2016. http://exa.ec/

Angwin, Julia, Savage Charlie, Larson Jeff, Moltke Henrik, Poitras Laura y Risen James. *"AT&T Helped U.S. Spy on Internet on a Vast Scale"* The New York Times. Publicado el 15 de Agosto de 2015. Último acceso el 17 de Julio de 2016. http://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html?_r=0

ARCOTEL. (a) Techos tarifarios. 2015a. Último acceso el 15 de abril de 2016 de http://www.arcotel.gob.ec/servicio-movil-avanzado-sma/

_____. (b) Internet, boletín estadístico del sector de telecomunicaciones. 2015b. Último acceso el 15 de Abril de 2016. http://www.arcotel.gob.ec/wp-content/uploads/2015/11/Boletin6.pdf

Asamblea Nacional Constituyente. *Constitución Política de la República del Ecuador*. Quito: 2008. Último acceso el 14 de febrero de 2016. http://www.asad2l usfq mbleanacional.gov.ec/documentos/constitucion_de_bolsillo.pdf

_____. *Ley Orgánica de Comunicación*. Quito: 2013. Último acceso el 14 de febrero de 2016.

http://www.asambleanacional.gob.ec/es/system/files/ley_organica_comunicacion.pdf

Carpintero, F. *La Cabeza de Jano*. Cádiz: Servicio de Publicaciones de la Universidad de Cádiz, 1989.

Carrión, Fernando. "Boletín: Debatir el presupuesto nacional desde la seguridad ciudadana." (Editorial). En *Programa de Estudios de la Ciudad*. Publicado en Mayo de 2015. Quito: FLACSO sede Ecuador. 2005. Último acceso el 2 de Febrero de 2016. http://hdl.handle.net/10469/2487

Deng, F. *Sovereignty as Responsibiliy and Accountability*. Washington: Brookings Institute, 1995.

Diario *El Comercio*. "Mayor competencia en telefonía móvil genera expectativa en Ecuador." 2014. Último acceso el 20 de Enero de 2016. http://www.elcomercio.com/actualidad/competencia-telefonia-movil-ecuador.html

Diario *El Universo*. "Tuenti es nueva marca de la operadora Otecel." Publicado el 16 de julio de 2015, último acceso el 20 de Enero de 2016. http://www.eluniverso.com/noticias/2015/07/16/nota/5021320/tuenti-es-nueva-marca-operadora-otecel.

Díaz de Terán Velasco, M. Cruz. "Seguridad, Desarrollo y Derechos de Tercera Generación: El caso de la libertad Informática." En *Seguridad, defensa y desarrollo en el contexto internacional actual*, editado por Eugenia López-Jacoiste Díaz (coordinadora), 111-124. Pamplona: Universidad de Navarra, 2010.

Dixon-Thayer, Denelle. "Get Smart On International Data Privacy Day," En *The Mozilla Blog*, Publicado 27 de Enero, 2015. Último acceso el 15 de Enero de

2016. https://blog.mozilla.org/blog/2015/01/27/get-smart-on-international-data-privacy-day/

Domestic Surveillance Directorate. "Surveillance Techniques: How Your Data Becomes Our Data." Último acceso el 15 de Enero de 2016. https://nsa.gov1.info/surveillance/

El País, EFE Economía, *Latinoamérica contará con 26 nuevos satélites en 2017*, Publicado el 5 de Septiembre de 2013, último acceso el 19 de febrero de 2016. http://economia.elpais.com/economia/2013/09/05/agencias/1378406754_112370.html

Fraga, Manuel. *Guerra y conflicto social*. Instituto de Estudios Políticos. 1962

Herz, J. "Idealist Internationalism and the Security Dilemma". En *World Politics*, vol. 2, no.2 (171-201), at p.157. Cambridge: Cambridge University Press, 1950.

Instituto Ecuatoriano de Propiedad Intelectual. *Software Libre: Política Pública y alternativa para defenderse del espionaje cibernético*. Publicado el 1 de Octubre de 2015. Último acceso el 15 de Febrero de 2016. http://www.propiedadintelectual.gob.ec/software-libre-politica-publica-y-alternativa-para-defenderse-del-espionaje-cibernertico/

Jervis, R. "Cooperation Under the Security Dilemma". En *World Politics*, vol. 30, no.2 (167–214), 1978.

Keohane, Robert O. *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton University Press, 1984

Larrea, Gustavo. (a) *Seguridad, Soberanía, Democracia y Política Exterior del Ecuador*. Quito: Ministerio de Relaciones Exteriores, Comercio e Integración, 2008a.

_____. (b) *Hacia una nueva Política de Seguridad Interna y Externa*. Quito: Ministerio Coordinador de Seguridad Interna y Externa. Seguridad, Soberanía y Democracia, Siglo XXI, 2008b.

LATSAT, *Congreso Latinoamericano Satelital de Comunicaciones y Radiofusión*, México, 18 y 19 de mayo, 2016. Ultimo acceso el 5 de Marzo de 2016. http://www.latsat-congreso.com/es

Lee Timothy. "Here's everything we know about PRISM to date." En *The Washington Post*, Publicado el 12 de Junio, 2013. Último acceso el 5 de Enero, 2016. https://www.washingtonpost.com/news/wonk/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/

López, Eugenia. "Seguridad humana y seguridad internacional: elementos clave para la paz." En *Seguridad, defensa y desarrollo en el contexto internacional actual*, editado por Eugenia López-Jacoiste Díaz (coordinadora), 186-187. Pamplona: Universidad de Navarra, 2010.

Megías Quirós, J.J. *Sociedad de la Información*, 2000.

Ministerio de Finanzas del Ecuador. *Informe de Transparencia y Rendición*. 2009. Revisado el 3 de Febrero de 2016. http://www.finanzas.gob.ec/wp-content/uploads/downloads/2012/08/Informe-Transparencia-y-Rendici%C3%B3n-de-Cuentas-2009.pdf

_____. *Informe de Transparencia y Rendición*. (2011, 2012, 2013, 2014). Revisado el 3 de Febrero de 2016. http://www.finanzas.gob.ec/

Ministerio de Finanzas del Ecuador. Presupuesto General del Estado Consolidado por Entidad Gastos. 2016. Extraído el 22 de abril de 2016 http://www.finanzas.gob.ec/wp-content/uploads/downloads/2014/12/13B.CN_Por-EntidadGastos.pdf

Moles Plaza R.J. *Derecho y control en Internet: La regularidad de Internet*, 22. Barcelona: Ariel, 2004.

Morgenthau, Hans. *Política entre las naciones: La lucha por el poder y la paz*, 41. Buenos Aires: Grupo Editor Latinoamericano, 1986.

ONU. *Carta de las Naciones Unidas*. Último acceso el 18 de Abril de 2016. http://www.un.org/es/sections/un-charter/chapter-i/index.html

_____. *La Declaración Universal de Derechos Humanos*. Último acceso el 18 de Abril de 2016. http://www.un.org/es/universal-declaration-human-rights/

_____. *Responsabilidad de proteger*. Último acceso el 2 de Marzo de 2016. http://www.un.org/es/preventgenocide/adviser/responsibility.shtml

Organización de los Estados Americanos, "Declaración sobre Seguridad en las Américas" (declaración presentada en la *Conferencia Especial Sobre Seguridad*, México, 27-28 de octubre de 2003. https://www.oas.org/es/ssm/CE00339S03.pdf

Pérez-Luño, A.E. *La tercera generación de derechos humanos*. Madrid: Thomson Aranzadi, Navarra, 2006.

Popovski, Vesselin. *World Religios and Norms of War*. Editado por Gregory M. Reichberg and Nicholas Turner. Tokyo: United Nations University Press, 2009.

Roldos, Léon. "¿Son pre asignaciones?, ¿o qué?" En *Diario El Comercio*. Publicado el 6 de Mayo del 2016. Último acceso el 6 de mayo de 2016. http://www.elcomercio.com/opinion/son-preasignaciones.html

Rousseau, J.J. El Contrato Social o Principios de Derecho Político. Traducido por Eduardo Velarde. París: Garnier Hermanos, 1910.

United Nations Trust Fund for Human Security. "Dependencia de Seguridad Humana, Enfoque basado en la seguridad humana." En *El concepto de seguridad humana* .New York. Último Acceso el 21 de Febrero del 2016. http://www.un.org/humansecurity/es/content/el-concepto-de-seguridad-humana

Velasco JJ. Blog oficial de Telefónica. Movistar, O_2, vivo; son marcas pertenecientes a telefónica. En Ecuador es más conocida como Movistar.2003. Publicado el 23 de Julio de 2013. Último acceso el 17 de abril de 2016. http://blogthinkbig.com/telstar-1-historia/

REFERENCIA DE TABLAS:

Tabla 1: La tabla fue realizada por el autor.

Tabla 2: Agencia Espacial Civil Ecuatoriana, EXA, Revisado el 7 de Marzo de 2016. http://exa.ec/

Tabla 3: Ministerio de Finanzas del Ecuador. 2009. Informe de Transparencia y Rendición. Último acceso el 3 de Febrero de 2016. http://www.finanzas.gob.ec/wp-content/uploads/downloads/2012/08/Informe-Transparencia-y-Rendici%C3%B3n-de-Cuentas-2009.pdf

Tabla 4: Ministerio de Finanzas del Ecuador. 2011, 2012, 2013, 2014. Informe de Transparencia y Rendición. Último acceso el 3 de Febrero de 2016. http://www.finanzas.gob.ec/