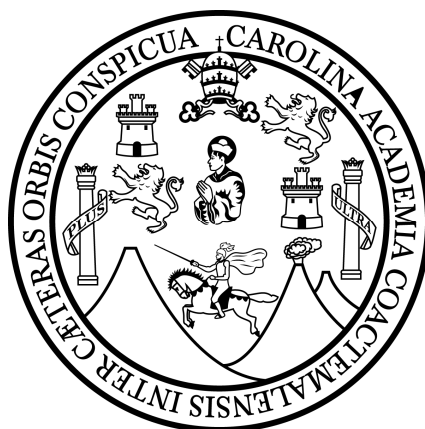


UNIVERSIDAD SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
ESCUELA DE ESTUDIOS DE POSTGRADO
DOCTORADO EN SEGURIDAD ESTRATÉGICA



Tesis doctoral

**Integración de las bases de datos de los Órganos de Seguridad
del Estado como modelo para la prevención de la delincuencia y
promoción de las denuncias**

César Augusto Cabrera Leonardo

Guatemala, febrero de 2016



USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala

**MIEMBROS DE JUNTA DIRECTIVA
FACULTAD DE CC. JJ. Y SS.
USAC**

DECANO

MSc. Avidán Ortiz Orellana

VOCAL I

Lic. Luis Rodolfo Polanco Gil

VOCAL II

Licda. Rosario Gil Pérez

VOCAL III

Lic. Juan José Bolaños Mejía

VOCAL IV

Br. Jhonathan Josué Mayorga Urrutia

VOCAL V

Br. Freddy Noé Orellana Orellana

SECRETARIO

Lic. Daniel Mauricio Tejeda Ayestas





USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala

TRIBUNAL EXAMINADOR

Dr. Luis Fernando Ruíz Ramírez
Presidente

Dr. Aníbal González Dubón
Vocal

Dr. Saúl González Cabrera
Secretario

CONSEJO ACADÉMICO DE ESTUDIOS DE POSTGRADO

DECANO: MSc. Avidán Ortiz Orellana

DIRECTOR: MSc. Luis Ernesto Cáceres Rodríguez

VOCAL: Dr. René Arturo Villegas Lara

VOCAL: Dr. Luis Felipe Sáenz Juárez

VOCAL: MSc. Ronaldo Porta España



Guatemala, 12 de abril de 2016

Mtro. Luis Ernesto Cáceres Rodríguez
Director de la Escuela de Estudios de Postgrado,
Facultad de Ciencias Jurídicas y Sociales
Universidad de San Carlos de Guatemala.

Señor director:

Por la presente, hago constar que he realizado la revisión de los aspectos de redacción y ortografía de la tesis:

**INTEGRACIÓN DE LAS BASES DE DATOS DE LOS ÓRGANOS DE
SEGURIDAD DEL ESTADO COMO MODELO PARA LA PREVENCIÓN DE
LA DELINCUENCIA Y PROMOCIÓN DE LAS DENUNCIAS**

Esta tesis fue presentada por el MSc. César Augusto Cabrera Leonardo del Doctorado en Seguridad Estratégica, de la Escuela de Postgrado de la Facultad de Ciencias Jurídicas y Sociales, de la Universidad de San Carlos de Guatemala.

En tal sentido, considero que, después de realizadas las correcciones indicadas, la tesis puede imprimirse.

Atentamente,


Dra. Gladys Tobar Aguilar
Revisora
Colegio Profesional de Humanidades
Colegiada 1450


Gladys Tobar Aguilar
Colegiada 1450



USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala

D.E.E.P. ORDEN DE IMPRESIÓN

LA ESCUELA DE ESTUDIOS DE POSTGRADO DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA, Guatemala, tres de mayo del dos mil dieciséis.-----

En vista de que el MSc. César Augusto Cabrera Leonardo, aprobó examen privado de tesis en el **Doctorado en Seguridad Estratégica**, lo cual consta en el acta número 3-2016 suscrita por el Tribunal Examinador y habiéndose cumplido con la revisión gramatical, se autoriza la impresión de la tesis titulada **“INTEGRACIÓN DE LAS BASES DE DATOS DE LOS ÓRGANOS DE SEGURIDAD DEL ESTADO COMO MODELO PARA LA PREVENCIÓN DE LA DELINCUENCIA Y PROMOCIÓN DE LAS DENUNCIAS”**. Previo a realizar el acto de investidura de conformidad con lo establecido en el Artículo 21 del Normativo de Tesis de Maestría y Doctorado.-----

“ID Y ENSEÑAD A TODOS”



MSc. Luis Ernesto Cáceres Rodríguez
DIRECTOR DE LA ESCUELA DE ESTUDIOS DE POSTGRADO



Ciudad Guatemala, 29 de octubre de 2015

Señor

Director de la Escuela de Estudios de Postgrado

Facultad de Ciencias Jurídicas y Sociales

Universidad de San Carlos de Guatemala

M Sc Luis Ernesto Cáceres Rodríguez

Señor Director:

Es ocasión distinguida dirigirme a usted para informar que he revisado el informe final de tesis del Maestro CÉSAR AUGUSTO CABRERA LEÓNARDO, la cual se titula: ***Integración de las bases de datos de los Órganos de Seguridad del Estado para prevenir actos delincuenciales y fortalecer la cultura de denuncia.***

Al respecto, advierto que esta propuesta identifica como problema de investigación la inadecuada u obsoleta captación, manejo y distribución e interpretación de datos e información que se recibe en las distintas instituciones estatales.

La inseguridad que actualmente se vive en Guatemala es una evidencia de que el Estado no ha cumplido a cabalidad el mandato constitucional, a pesar de que, según reconoció la Alta Comisionada de las Naciones Unidas para los Derechos Humanos, Navi Pillay, en su informe en el marco del 22 Período de Sesiones del Consejo de Derechos Humanos de la ONU, y cito: «La tasa de muertes violentas ha mantenido una tendencia a la baja desde 2010, pero persisten altos

índices de violencia e impunidad, incluyendo crímenes atroces en contra de mujeres y niños.»

La realidad señalada por la Comisionada de la ONU, en buena medida, es resultado de la debilidad estatal, la improvisación, la falta de sistematización, la escasa profesionalización de muchas personas que tienen a su cargo la conducción de la seguridad, la falta de actualización permanente, el manejo de tecnología inadecuada, la visión cortoplacista y de contingencia que ha sido el común denominador de este tema crucial para la vida en paz y tranquilidad de los ciudadanos.

Además, el uso de prácticas empíricas y obsoletas para la garantía de la seguridad. Esas fallas en el desempeño estatal han sido evidenciadas y objeto de estudios, análisis y reflexiones que, a partir de los *Acuerdos de Paz*, propiciaron una reconfiguración de la seguridad y una modernización de las instituciones encargadas de la seguridad que apenas comienza su fase de consolidación.

Sin embargo, hay avances significativos porque, a partir de la *Ley Marco del Sistema Nacional de Seguridad* (decretada en 2008) y de la *Política Nacional de Seguridad* (establecida en 2012), quedó diseñada una ruta posible para que el Estado pueda cumplir, de mejor manera, con sus deberes constitucionales en materia de seguridad. Muchos avances aún están en fase de teoría, pero a partir de la *Política Nacional de Seguridad*, adquieren visos de ejecución.

Desde el punto de vista informático, el tema es de suma importancia porque si se mejora este aspecto de la información, será posible que los procesos judiciales puedan agilizarse y, en consecuencia, proveer de una justicia pronta y expedita. En tal orientación, permitirá el acceso e integración a la información de los diferentes organismos e instituciones estatales que manejan datos de actos delincuenciales; por ejemplo, las denuncias, presencia de maras y crimen organizado en ciertos sectores del país, etc. «La información exacta es una guía esencial para la acción. Cada organización necesita sistemas para recopilar y almacenar datos, rastrear los

indicadores clave del desempeño, identificar y diagnosticar los problemas y reportar la información crítica para la estrategia.»

Uno de los pilares más importantes de la informática es tratar de integrar la información de toda índole para hacer eficaces los procesos y simplificar los mecanismos de búsqueda de información.

Los aspectos que inciden en el tema de la seguridad son muy variados; por eso, el Sistema Nacional de Seguridad (SNS) ha designado a las instituciones encargadas de cada aspecto específico; no obstante, todas deben funcionar de manera coordinada; sin embargo, no puede consolidarse esa integración institucional sin la integración de los datos de los Órganos de Seguridad del Estado.

La hipótesis formulada por el Maestro CÉSAR AUGUSTO CABRERA LEONARDO ha sido demostrada en el sentido de la eficacia de la unificación del sistema de denuncias, en un solo sistema, para que todas las instituciones del Sistema Nacional de Seguridad puedan aprovecharse de este mismo y a la vez retroalimentarlo.

En la tesis se propone una reorganización de la estructura de las denuncias que se plantean a las distintas instituciones gubernamentales agrupadas en el SNS; o sea, plantear un sistema de almacenamiento de datos (*data-warehouse*), de tal forma que este permita compartir datos (*e-data*) entre Ministerio Público, Procuraduría de Derechos Humanos, Policía Nacional Civil, Juzgados de Paz y de Familia, Bufetes Populares, Procuraduría General de la Nación, para dar un mayor seguimiento a todo tipo de denuncia y poder relacionar los casos para obtener resultados concretos en esta materia.

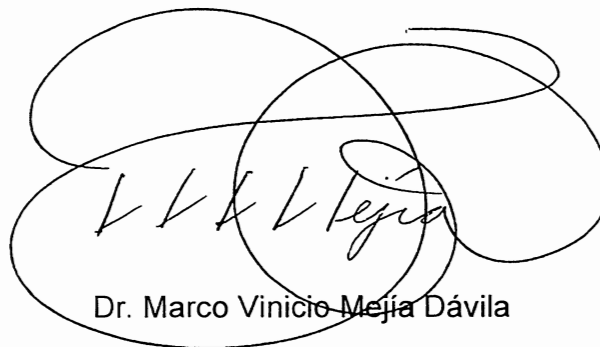
En consecuencia, al implementar un sistema que optimice los procesos, se estará contribuyendo a que haya justicia y, por supuesto, mayor seguridad. Al darse esa mejora, la consulta de los casos podrá ser inmediata, logrando reducir los tiempos en brindar respuesta a las personas afectadas. La relación entre casos de

diferentes instituciones podrá, entre otros aspectos, brindar mejor información. Para esto, también, se verificará si el denunciado ha cometido hechos ilícitos de cualquier tipo que pudieran ser vinculantes a un nuevo proceso.

En esta tesis se arribó a la conclusión de que al integrar la información sobre actos delincuenciales en un *data warehouse*, se logrará fortalecer de manera eficaz la seguridad ciudadana ante la delincuencia y, por añadidura, fortalecer la cultura de denuncia. El Doctorando ha analizado de manera crítica los métodos que se emplean actualmente en dicho proceso; así, también, la percepción de la población sobre cómo se maneja actualmente una denuncia.

Presento de manera entusiasta mi dictamen de aprobación de este informe final de investigación de tesis, por lo que debe continuarse con el trámite académico y señalar día y hora para su defensa, y así se le otorgue el título de Doctor en Seguridad Estratégica.

Sin otro particular, lo saludo con las muestras de la más alta consideración.



Dr. Marco Vinicio Mejía Dávila

Doctor en Filosofía y Doctor en Derecho

Índice

Introducción	3
Capítulo I	16
1. La información	16
1.1 Dato	18
1.2 Procesamiento de los datos	23
1.3 Matrices para procesamiento de datos	29
1.4. El Data warehouse	31
1.5 Características de la información	33
1.6 Clases de información	34
1.7 Teoría de la información	35
Capítulo II	46
1. Inteligencia de Estado	46
2. Los elementos de la Inteligencia en Guatemala	58
2.1. Inteligencia	58
2.2. Sistemas de Inteligencia	58
2.3. Contrainteligencia cibernética	59
2.4. Gestión del Conocimiento y Servicios de Inteligencia	63
3. Esbozo histórico de la Inteligencia en Guatemala	65
3.1. El período liberal	65
3.2. El gobierno de Manuel Estrada Cabrera	67
3.3. Después de Estrada Cabrera	69
3.4. Después de 1954	80
3.5. La llegada de la Informática	88
3.6. En la actualidad	90
Capítulo III	94
1. La denuncia	94
1.1. Concepto	94
1.2. Por qué es importante denunciar	95
1.3. ¿Qué implica una cultura de denuncia?	96
2. ¿Se puede mejorar el sistema de denuncia automatizando digitalmente los procesos?	96
3. Modernización de la tecnología de acopio de denuncias	100
3.1. Virtudes en las implementaciones de base de datos	101
3.2. ¿Qué es una base de datos?	102

3.2.1. ¿Para qué sirve una base de datos?	103
3.2.2. Tipos de bases de datos	105
3.2.3. La base de datos para las denuncias	107
3.2.4. La estructura de una base de datos	108
3.2.5. Equipo	114
3.2.6. Funcionamiento	114
4. Procesos obsoletos de las denuncias actuales	118
4.1. Crítica al sistema de denuncias del Ministerio Público	119
4.2. Crítica al sistema de denuncias de la Policía Nacional Civil	120
5. Codificación de seguridad para el resguardo de la información para que solo las instituciones designadas y el personal autorizado puedan tener acceso a la información	121
6. Integración del Sistema de Denuncias de todas las instituciones estatales vinculadas con el Sistema Nacional de Seguridad	126
7. Creación de un Reglamento y Código Ético que deberán regir el uso de la información generada por este sistema unificado de información	127
8. Capacitación y tecnificación del personal encargado de recibir las denuncias	127
9. Campaña nacional de educación para el acceso al sistema de denuncias	128
10. Concepto de una denuncia a nivel social	129
11. Cifra negra de la criminalidad	130
12. Encuestas de victimización	132
13. La inversión	132
 Capítulo IV	 135
1. Internet, desobediencia civil y la resistencia del pueblo	135
1.1. De la “Primavera árabe” a la “Primavera guatemalteca”	135
2. ¿Qué es la desobediencia civil?	144
3. Características de la desobediencia civil	146
4. De la desobediencia civil al activismo político en la Internet	148
5. La información y los derechos humanos	152
6. Habeas Data y protección legal de la información	160
 Conclusiones	 165
 Bibliografía	 168

Introducción

Algunas personas ancianas afirman con nostalgia que en «los tiempos de don Jorge», refiriéndose a Jorge Ubico (1930 – 1944), la seguridad de las personas estaba garantizada por el gobierno y que su violación no era un asunto alarmante. Aparentemente, la gente vivía con mayor tranquilidad y podía salir a cualquier hora del día, o de la noche, sin temor a perder la vida o sufrir actos violentos. Y que, cuando se alteraba la seguridad, «la justicia» actuaba con severa drasticidad; sin mucho trámite, al infractor se le condenaba a muerte. Una de estas modalidades era la «Ley Fuga».¹ Además, la ejecución de los fusilamientos se divulgaba por los medios de comunicación; era un espectáculo público para que sirviera de ejemplo a la población y, de tal manera, se abstuviera de delinquir.² Esa percepción de la gente que vivió épocas de autoritarismo no corresponde a las circunstancias que vivimos actualmente, en que las amenazas, las vulnerabilidades y los riesgos son de otra naturaleza. «Lo que a veces no nos cuentan los abuelos, es a costa de qué se tenía esa seguridad. Esa ficción de seguridad, pues la represión inmanente que la generaba, al final resultó ser lo que socavó los catorce años de dictadura y que pretendían ser al menos, dieciocho, tras varias alteraciones a la Constitución

¹ «La ley fuga, otra de las formas de violencia institucional aplicadas por el gobierno de Jorge Ubico, consistía en asesinar por la espalda a los delincuentes y a los prisioneros políticos, aduciendo su intento de escapatoria. Al igual que la tortura, la ley fuga de 1931 a 1934 se emplea cotidianamente contra los delincuentes en el interior de la República, siendo la encargada de su aplicación la llamada Guardia Rural. Pero después de 1934 se aplica también contra los presos políticos y principalmente contra los opositores del entonces gobernante». Locón Solórzano, Agustín Haroldo. *La violencia durante el Gobierno de Jorge Ubico*. Tesis. Escuela de Historia, Universidad de San Carlos de Guatemala, mayo 1997, pág. 76.

² *Ibidem*, pág. 79.

liberal que estuvo vigente hasta 1944.»³ También, debe tenerse en cuenta que la población en esa época era considerablemente menor que en la actual. Si antes se vivía bajo regímenes dictatoriales ahora nos esforzamos por transitar hacia una democracia que, aunque imperfecta, se ha construido a base de muchos esfuerzos, muertos, dolor y tragedia.

No obstante lo anterior, la gente tenía confianza en que, de alguna manera, su seguridad, y sobre todo su vida, estaban garantizadas, siempre y cuando no se intentara rebelión ni se cuestionara el sistema imperante; en consecuencia, confiaban en las autoridades que la brindaban, a pesar de que eso implicara la restricción de su libertad.

¿Qué cambió esa situación en la cual se aceptaba todo lo que sus gobernantes decidían? Precisamente, el planteamiento social de recuperar la libertad, a sabiendas de que no hay libertad sin riesgo. A imitación de la sociedad norteamericana que manifestó su desacuerdo contra las guerras que emprendía su gobierno, especialmente la impuesta contra Vietnam, los estadounidenses se resistieron al *status* bélico. Lo hicieron por medio de un movimiento que tuvo los *slóganes* que articularon a gran parte de la sociedad, sobre todo a los jóvenes, y consistieron en «paz y amor» y «amor, no guerra». Pronto se convirtió en un movimiento pacifista, libertario, anti-guerrero y contracultural que remarcó su rechazo contra la guerra; sobre todo antinuclear, a partir de la experiencia de Hiroshima y Nagasaki, en 1945, donde después de las bombas lanzadas, se

³ Álvaro Castellanos Howell, *Elperiódico*, 11-2-2014.

estima que murieron 220,000 personas; 110,000 de ellas muertas como consecuencia directa del bombardeo y el resto como secuela de las radiaciones emitidas por los artefactos nucleares.

¿Qué hizo el gobierno estadounidense y el propio sistema para contrarrestar tales protestas, manifestaciones antiguerreristas, contraculturales y antisistema? Sencillamente tomó todos los símbolos y signos de tal movimiento y los trastrocó; es decir, los resemantizó para neutralizarlos; les asignó valores contrarios a los originales y los volvió moda. Al símbolo principal de «paz y amor», le dieron una connotación sexual; la anti solemnidad la volvieron moda al popularizar las llamadas *t-shirts* y los pantalones *jeans*. Además, los explotaron comercialmente, apoyados por un montaje publicitario y estratégico que copó, prácticamente, todas las instancias mediáticas. El *rock* de protesta lo banalizaron propiciando en las bandas la exaltación, también, de lo sexual y romántico. Esa fue la respuesta del sistema norteamericano en su país, porque allí era imposible aplastar ese movimiento por la vía de la guerra o la represión directa. Al ciudadano común y corriente, asediado por la carga publicitaria, psicológica e ideológica, no le quedó más que rendirse ante la presión y aceptar esos nuevos símbolos como parte de los nuevos tiempos. Fue una solución realmente astuta la del sistema, la del gobierno y los poderes fácticos estadounidenses. Pero fuera de su país ocurrió algo distinto. Dejaron que se imitaran las modas, la liberación sexual y otros aspectos del movimiento *hippie* que afloró, pero obligaron a los gobiernos latinoamericanos a no permitir la insurrección ni movimiento alguno que implicara una amenaza estratégica para ellos. Fue una jugada del gobierno estadounidense

que, con el argumento de impedir la intromisión del comunismo en los países que orbitaban en su influencia, los llevó a presionarlos, y la mayoría se rindió ante sus imposiciones.

Después de ese período se dio un paso fundamental en nuestra historia: el primer ensayo de la democracia, como rectora de la institucionalidad, que duró tan solo diez años y abarcó los gobiernos revolucionarios de Juan José Arévalo y Jacobo Árbenz Guzmán (1944-1954). Uno de los aportes fundamentales de ese periodo fue la *Constitución de la República*, decretada el 11 de marzo de 1945.

En 1954 se rompió con esa modalidad gubernamental. A partir de allí se instauraron regímenes autoritarios que dieron paso a una seguridad basada en la llamada Doctrina de Seguridad Nacional (DSN), cuyo objetivo primordial fue la lucha contrainsurgente, basada en dotar de seguridad a las instituciones estatales y gubernamentales con el argumento de no permitir que el comunismo tomara el poder; tal objetivo comenzó a configurarse en 1965, cuando el presidente Lyndon B. Johnson incrementó la invasión norteamericana en Vietnam y luego de derrocar, en las Antillas, al gobierno dominicano.⁴

La DSN, tal como se aplicó en Guatemala no estuvo enfocada en la seguridad de la población, sino en la seguridad del Estado.⁵

⁴ Estas fueron las palabras de Johnson: «Una revolución en el interior de un país es algo que le concierne sólo a dicha Nación [...] y se convierte en una materia de acción hemisférica sólo cuando su objeto es el establecimiento de una dictadura comunista.» (Citadas por Jorge A. Tapia Valdés, *El terrorismo de Estado*, Editorial Nueva Imagen, México, 1980, Pág. 51).

⁵ La Inteligencia militar en Guatemala se diseñó «con base en la Doctrina de Seguridad Nacional (DSN) aplicada en Latinoamérica dentro del conflicto Este-Oeste bajo los parámetros de la guerra total del Estado contra el comunismo. Este sistema no tuvo novedades en relación con los modelos

Posteriormente, se desató la guerra de los 34 años y 10 meses, según la Comisión del Esclarecimiento Histórico, y que eufemísticamente fue denominada como «conflicto armado interno».

Al terminar tal confrontación, vinieron los *Acuerdos de Paz*, dentro de los cuales el *Acuerdo de Paz Firme y Duradera* se firmó el 29 de diciembre de 1996; estos acuerdos posibilitaron una nueva visión de convivencia social. A partir de allí, se dio paso a un nuevo enfoque de la seguridad basado en la Seguridad de la Nación.

Ahora sabemos que la seguridad es un factor muy importante para la convivencia, pero que no puede estar sujeta a la limitación de la libertad que es un principio inalienable garantizado en la propia *Constitución Política de la República de Guatemala* (Artículo 3º): «En Guatemala todos los seres humanos son libres e iguales en dignidad y derechos.»

Los avances científicos y tecnológicos han dotado a la sociedad democrática de muchos recursos que ahora permiten una nueva manera de convivencia, pero también suponen peligros y amenazas nuevas. El mismo ejercicio de los derechos humanos ha dotado a la sociedad de una nueva visión sobre la sociedad, la convivencia y la necesidad de respetar los derechos fundamentales de los seres humanos. En la misma *Ley Marco del Sistema Nacional de Seguridad* (Capítulo II, Artículo 2, inciso b), se establece que «La Seguridad Democrática es la acción del Estado que garantiza el respeto, promoción y tutela de la seguridad, al mismo

de otros países latinoamericanos, inscritos en la política contrainsurgente.» (Comisión para el Esclarecimiento Histórico, *Guatemala memoria del silencio*, Tomo II, Guatemala. 1999, Pág. 74).

tiempo que el pleno ejercicio de los derechos humanos, mediante la creación de condiciones que le permita a la persona su desarrollo personal, familiar y social en paz, libertad y democracia, conforme a lo establecido en el Tratado Marco de Seguridad Democrática en Centroamérica.»

No obstante los avances que se han logrado en materia de seguridad y en la creación de instituciones especializadas en brindarla y garantizarla, la población aun no recupera la confianza en sus instituciones; en consecuencia, se abstiene con mucha frecuencia de acudir a ellas; sobre todo, se limita en su derecho a denunciar las amenazas contra su seguridad. Una de las razones para esta manera de actuar ciudadana es que las instituciones, cuando se les requiere, en general, no actúan con la debida celeridad, como consecuencia de su descoordinación y de las prácticas obsoletas en los sistemas de captación de denuncias, de almacenamiento de la información y disponibilidad de la misma; como resultado, en la deficiente disposición de los insumos necesarios para «la prevención de los riesgos, control de las amenazas a la seguridad y la reducción de las vulnerabilidades que impidan al Estado cumplir con sus fines.»⁶ Por eso, la recuperación de la confianza ciudadana ha sido manifestada como una necesidad de Estado y ha sido plasmada en la *Política Nacional de Seguridad* (Pág. iv): «Es necesario recuperar la confianza de la población en el Estado y mejorar la coordinación entre sus instituciones, para generar las capacidades requeridas y disminuir las causas que provocan inseguridad y violencia, alojadas en el tejido social. Solamente un Gobierno democrático tiene la legitimidad para hacerlo a la

⁶ *Ley Marco del Sistema Nacional de Seguridad*, Capítulo III, Artículo 4.

par de un Sistema de Seguridad eficiente que produzca las competencias requeridas para enfrentar este desafío.» Una de estas competencias es la institucionalización de un sistema de información ágil y en coordinación interinstitucional; que sea eficiente a partir de la recolección de los datos y de su procesamiento para transformarlos en información confiable y efectiva para sustentar una Inteligencia Estratégica de Estado⁷ que permita, sobre todo, prevenir cualquier amenaza a la seguridad ciudadana. Como dato, debemos tener presente que, hacia 2006, «el costo global de la violencia, en Guatemala asciende a Q 17,900.4 millones equivalente a US\$ 2,386.7 millones que, en términos del PIB, representa 7.3%»,⁸ dato que el PNUD calcula conservador.

La recuperación de la confianza ciudadana en las instituciones es fundamental. Uno de los aspectos, entre muchos, que contribuiría en buena medida a ese logro sería la eficiencia en la captación de denuncias que se realizan en las distintas instituciones del Estado, en particular en las entidades que conforman el Sistema Nacional de Seguridad. En ese sentido, se requiere tener en cuenta que la falta de confianza ciudadana es resultado de la debilidad estatal, la improvisación, la falta de sistematización, la escasa profesionalización de muchas personas que tienen a su cargo la conducción de la seguridad, la falta de actualización permanente, el manejo de tecnología inadecuada, la visión

⁷ Según la *Política Nacional de Seguridad* (Pág. vi) la Inteligencia Estratégica de Estado es necesaria para: «Dotar al Estado de un Sistema Nacional de Inteligencia que a partir del análisis coyuntural y estructural pueda anticipar, prevenir, contener y enfrentar los diferentes riesgos, amenazas y vulnerabilidades que afecten la calidad de vida de las personas y proporcionar los elementos esenciales para la toma de decisiones ejecutivas.»

⁸ PNUD, *El costo económico de la violencia en Guatemala*, Guatemala, 2006, Pág. 62.

cortoplacista y de contingencia que ha sido el común denominador de este tema crucial para la vida en paz y tranquilidad de los ciudadanos; además, el uso de prácticas empíricas y obsoletas para la garantía de la seguridad. Y, ahora como una amenaza que no se había detectado en toda su magnitud destructiva, la corrupción. Esas fallas en el desempeño estatal han sido objeto de estudios, análisis y reflexiones que, a partir de los *Acuerdos de Paz*, propiciaron una reconfiguración de la seguridad y una modernización de las instituciones encargadas de la seguridad que apenas comienza su fase de consolidación. Sin embargo, hay avances significativos. A partir de la emisión de *Ley Marco del Sistema Nacional de Seguridad* (decretada en 2008) y de la *Política Nacional de Seguridad*⁹ (formulada en 2012), se diseñó una ruta posible para que el Estado pueda cumplir, de mejor manera, con sus deberes constitucionales en materia de seguridad. Muchos avances aún están en fase de teoría y planificación, pero a partir de la *Política Nacional de Seguridad*, adquieren visos de ejecución.

Esta investigación tiene como ejes la verificación hipotética de la estructura de las denuncias que se plantean ante las distintas instituciones estatales, en especial las agrupadas en el Sistema Nacional de Seguridad (SNS)¹⁰ y, además,

⁹ «La Política Nacional de Seguridad se orienta a construir las condiciones para que las personas se sientan seguras, libres de violencia y temor, confiadas en alcanzar sus aspiraciones individuales y colectivas. Asimismo, tiene como fin integrar los esfuerzos de todo el país en un propósito común: lograr el desarrollo integral, fortalecer la democracia y superar las desigualdades sociales, para edificar una “Guatemala Segura y Próspera”.» (Otto Fernando Pérez Molina, en *Política Nacional de Seguridad*).

¹⁰ Según el artículo 3 de la *Ley Marco del Sistema Nacional de Seguridad*, el Sistema Nacional de Seguridad «consiste en el marco institucional, instrumental y funcional del que dispone el Estado para hacer frente a los desafíos que se le presenten en materia de seguridad, mediante acciones de coordinación interinstitucional al más alto nivel y sujeta a controles democráticos. Comprende los ámbitos de seguridad interior y exterior.»

la propuesta de una reorganización; o sea, plantear un sistema de almacenamiento de datos (*data-warehouse*) de tal forma que este permita acopiar y compartir datos (*e-data*) entre Ministerio Público, la oficina del Procurador de los Derechos Humanos, Policía Nacional Civil, Organismo Judicial, Procuraduría General de la Nación y las entidades que conforman el Sistema Nacional de Seguridad, para dar un mayor seguimiento a todo tipo de denuncias y así poder relacionar los casos para obtener resultados concretos en esta materia. No está planteada como una opción utópica; por el contrario, está asentada en la realidad y evidenciando los factores necesarios para hacerla posible: costos humanos y económicos, esfuerzos institucionales, insumos tecnológicos, etcétera. En consecuencia, al institucionalizar un sistema que optimice los procesos de información, se coadyuvará para que la administración de justicia mejore su eficiencia. Ese factor contribuirá a proveer a los ciudadanos de mayor seguridad. Al darse esa mejora, la consulta de los casos podrá ser inmediata, lográndose reducir los tiempos en brindar respuesta a las personas afectadas y establecer un modelo de prevención de la delincuencia. La relación entre casos de diferentes instituciones podrá, entre otros aspectos, brindar información más amplia y segura. Para esto, también se verificará si el denunciado ha cometido hechos ilícitos de cualquier tipo que pudieran ser vinculantes a un nuevo proceso. Además de mejorar considerablemente la recolección de datos, habrá mayor celeridad para la provisión de información requerida por la ciudadanía.

En el primer capítulo de mi investigación advierto que cuando un conjunto de datos se examina de manera conjunta, en el marco de una teoría de la

información, se puede apreciar la información que contienen dichos datos. De otro modo, si únicamente se cuenta con datos aislados, estos pueden no incluir información relevante. Cuando los datos son agrupados, estructurados e interpretados, de manera conveniente, constituyen la base de información relevante que puede emplearse en la toma de decisiones o reducir la incertidumbre, además de poder efectuar cálculos.

En el segundo capítulo, abordo la Inteligencia de Estado. Sostengo que se requieren soluciones concretas para controlar y convertir en conocimiento útil la información que deben procesar las instituciones que conforman el Sistema Nacional de Seguridad, en interacción con el Sistema Nacional de Inteligencia. La integración de las bases de datos de estas entidades permitirá que el Consejo Nacional de Seguridad cuente con las informaciones, análisis, estudios o propuestas que permitan prevenir y evitar los peligros, amenazas o agresiones contra la independencia o integridad territorial de Guatemala, los intereses nacionales y la estabilidad del Estado de Derecho y sus instituciones. El uso de información pertinente e idónea para la toma de decisiones sobre una base firme es una constante histórica, por lo que realizo un esbozo histórico de la Inteligencia en Guatemala. Finalmente, en este apartado advierto que si la Inteligencia es el proceso sistemático de recolección, evaluación y análisis de información, la ContraInteligencia forma parte de la actividad de Inteligencia, cuya finalidad es detectar, localizar, neutralizar o evitar las acciones de Inteligencia desarrolladas por actores (nacionales o extranjeros) que representen amenazas o riesgos para los derechos y libertades de los ciudadanos, la soberanía, integridad y seguridad

del Estado o Nación, la gobernabilidad democrática, el ordenamiento constitucional o el Estado de Derecho.

El tercer capítulo lo dedico a la necesidad de mejorar el sistema de denuncias de hechos ilícitos para integrar el Sistema de Denuncias de todas las instituciones estatales, vinculadas o no con el Sistema Nacional de Seguridad. Debido a las deficiencias en los servicios judiciales, la ineficacia de la investigación criminal y la falta de participación ciudadana, en cuanto a la falta de denuncias ante instituciones como el Ministerio Público, la Policía Nacional Civil y los tribunales, se requiere determinar la cifra negra de la criminalidad, la cual se mide por los delitos no denunciados, los que no dan lugar a averiguación previa a pesar de haberse denunciado, los sufridos en un solo incidente, por una o varias víctimas, que se registran en una sola averiguación previa, y los que no se registran por deficiencias en el sistema estadístico oficial. Instrumentos como las denuncias y las encuestas de victimización proporcionarían información para prevenir la criminalidad. La carencia de una cultura de la denuncia, se puede deber a diversos factores como: la lentitud de los procesos de investigación, la falta de atención de las instituciones competentes, el desconocimiento de las víctimas sobre los procedimientos, y la desconfianza hacia las instituciones responsables de la seguridad ciudadana, entre otros. Entre los objetivos de promover esta “Cultura de la Denuncia” se encuentra la generación de mejores políticas públicas para la modificación de los procesos judiciales y la atención a las víctimas.

En el capítulo cuarto advierto que la falta de credibilidad en las instituciones públicas, la percepción de inseguridad y la generalización de la violencia, son situaciones anormales que amenazan gravemente o ponen en peligro inminente la gobernabilidad del Estado y del ordenamiento jurídico. Debido a que estas circunstancias no pueden ser afrontadas y superadas con los instrumentos que proporcionan la Constitución Política y las leyes del país, las personas pueden recurrir a medidas extraordinarias. Este es el sustento de la legítima defensa, es decir, repeler los actos ilegítimos contra la ciudadanía, debiéndose en todo caso mantener el principio de proporcionalidad, ya que los medios empleados para repeler las agresiones deben ser proporcionales a las circunstancias. Tanto la legítima resistencia del pueblo para la defensa de sus derechos, así como los derechos que se desprenden de la evolución incontenible de las tecnologías de la información pertenecen a una nueva generación de derechos humanos. Las autopistas de la información representan una vía abierta para mejorar la condición humana, para la libertad, la justicia, la igualdad y la paz mundiales, ya que acercan a las personas más allá de las fronteras y crean un entorno en el que la diferencia no es vista como un elemento amenazador. De ahí que los derechos humanos en el ciberespacio, por ser inherentes al ser humano aunque no figuren expresamente en la *Constitución Política de la República de Guatemala*, forman parte de los derechos de una nueva generación, los cuales deben ser promovidos y protegidos. De ahí que cada institución que regule o actúe en el ámbito de los sectores de la información y el conocimiento, deben esforzarse por promover el respeto de estos derechos y libertades, asegurando mediante medidas orientadas

tanto al ciberespacio como al mundo físico, su reconocimiento y observancia universal, es decir, por parte de proveedores de servicios, usuarios individuales, organizaciones privadas e instituciones públicas. Entre estas últimas se encuentran las entidades que en Guatemala integran tanto el Sistema Nacional de Seguridad así como el Sistema Nacional de Inteligencia.

Capítulo I

«La información lo es todo, en la guerra como en la paz, en la política como en la economía.»¹¹

1. La información

De manera muy general, la información es una estructura de datos; o sea, un conjunto de datos, que se relacionan entre sí; que tienen un contexto dentro del cual se implican. Si no se relacionan entre sí, si no están contextualizados dentro de un tema, objetivo, función o materia y, además, bien especificados, no constituyen información. Puedo contar con una cantidad enorme de datos, pero, si no me sirven para un fin específico, no constituyen información. Los datos se convierten en información cuando, dentro de un contexto determinado, puedo procesarlos, analizarlos, verificarlos y utilizarlos para la toma de decisiones. Por ejemplo, puedo tener los siguientes datos aislados:

1. Una persona juega billar.

2. Un taxi dejó frente a la sala el billar a una persona y le extendió una factura por Q. 75.00.

3. El supermercado vecino extendió una factura por Q. 50.

Esos datos, así como los enumeré, son solamente datos aislados que, al no relacionarlos (o procesarlos), no constituyen información. No obstante, al vincularlos dentro de un contexto, se convierten en elementos para crear información. Para el caso de esta investigación, al convertirlos en *e-data* (dato

¹¹ Zweig, Stefan, *Fouché*, Instituto Cubano del Libro, Ediciones Huracán, Cuba, 1999, Pág. 92.

electrónico) y alojarlos en un *data warehouse*,¹² me dicen: tal persona es sospechosa de haber cometido el crimen que investigo sobre un asesinato que ocurrió en tal sala de billar, porque estuvo allí a la hora del crimen; luego, al allanar su casa por orden judicial, en el bolsillo de la camisa se le encontraron las facturas que determinaron su compra en el supermercado y haber usado el taxi. Esos documentos me permiten saber la hora en la cual llegó, dónde tomó el taxi; la central de taxis me proporciona el número de teléfono desde el cual llamó, etc.; además, en su bolsa encontré un pedazo de tiza con que se frota la punta del taco de billar; el recubrimiento de cartulina de la tiza es de la misma marca de las que compra siempre el dueño del billar. Como resultado de esa incidencia, todos esos datos se convierten en información porque reunidos me permiten establecer la ubicación y la implicación del sospechoso en el crimen que investigo. Así, los datos se convierten en información en la medida en que consigo reunirlos, analizarlos, evaluarlos y me permiten tomar decisiones o, en este caso, orientar de manera más específica las pesquisas sobre el asesinato. Para redondear, «la **información** son datos que adquieren significado dentro de un contexto. La información puede consistir en datos primarios o datos manipulados a través de la

¹² El *data warehouse* consiste en una plataforma de *hardware* separada; o sea, puede ser una computadora (servidor) aparte que permita almacenar y concentrar información que luego se organizará, por medio de un *software* adecuado, para que pueda servir, en el caso del SNS, para recolectar datos e información que luego permita analizarlos y, de esa manera, darles seguimiento a procesos iniciados o por iniciar; servir de soporte para la prevención delincriminal, etc. En resumen, «Es la combinación de hardware, software especializado y datos.» (Dyché, Jill, *E-data*, Prentice Hall, Pearson Education S. A., Brasil, 2001, Págs. 35 y 36). Sirve de «repositorio» de la información que le llega de estaciones de trabajo individuales o institucionales y que podrá ser utilizada para el análisis y toma de decisiones. Para el caso del Sistema Nacional de Seguridad (SNS), que es el ámbito dentro del cual ubicaré esta investigación: centralizar la información.

suma, la resta, la división o cualquier otra operación que conduzca a una mayor comprensión de una situación.»¹³

¿De qué clase de información se ocupará esta investigación?

De la información necesaria para el efectivo desempeño de la Inteligencia de Estado, desde sus orígenes hasta la modalidad actual; para tal objetivo se hará un breve repaso histórico que nos servirá para entender de mejor manera la evolución de ese elemento importante en la seguridad estatal, primero, y luego en el enfoque actual de la Inteligencia orientada hacia la seguridad democrática o ciudadana.

¿Por qué es tan necesaria la información?

Porque es el elemento más importante para el desempeño de una Inteligencia de Estado.

¿Por qué debe ocuparse el Estado de las tareas de información estratégica? —teleología.

Esta investigación se realizará, en buena medida, sobre los siguientes pilares: el dato, el procesamiento de datos, la información en general, la teoría de la información y la Inteligencia de Estado (el conocimiento).

1.1 Dato

La etimología de la palabra dato es latina: *datum*, que significa: lo dado. Cuando se comenzó a utilizar este vocablo se refería, prácticamente, a cualquier objeto

¹³ Oz, Effy, *Administración de sistemas de información*, Thomson Learning, Segunda edición, México, 2001, Pág. 8.

dado; sin embargo, más tarde comenzó a usarse para referirse solo a aquellos elementos u objetos referidos a la información.

El dato surge como una respuesta a la necesidad que el ser humano tuvo, desde sus orígenes, de conocer su entorno y circunstancias; es decir, tener elementos que le brindaran la oportunidad de interrelacionarlos y, a partir de esa acción, obtener la información requerida para crear conocimiento que le permitiera su sobrevivencia. En ese sentido: «La más elemental de las decisiones precisó de datos, nociones, conocimiento del entorno ambiental y de sus habitantes, como de los riesgos y amenazas presentes y previsibles.»¹⁴

«Desde corrientes como el empirismo (Hume, Locke), se acepta que el dato es el hecho, la evidencia, las propiedades de la realidad externa a las que el hombre tiene acceso, más o menos directo, por vía sensorial. El dato es la unidad más simple en que se refleja el conocimiento: constituye la definición “más temprana”, menos elaborada de la realidad que pretendemos conocer.»¹⁵ Los sentidos que en la actualidad se le asignan a la palabra dato son innumerables; sin embargo, para efectos de esta investigación, el enunciado en este párrafo será el que la orientará en su modalidad de *e-data*.¹⁶

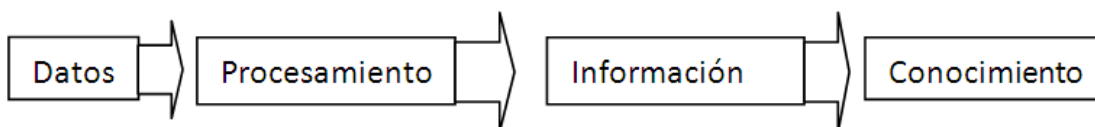
¹⁴ Cáceres G., José Raúl, en: <http://www.intelpage.info/web/externo/textos/estrategica.pdf>, consultado el 26-03-2014, a las 11:45 horas.

¹⁵ Gil Flores, Javier, *Análisis de datos cuantitativos. Aplicación al caso de los datos procedentes de grupos de discusión*, Tesis doctoral, Universidad de Sevilla, Facultad de Filosofía y Ciencias de la Educación, España, 1993, Pág. 20.

¹⁶ Utilizaré la terminología informática en inglés, para mejor comprensión, ya que en el ámbito académico se usa este idioma con preeminencia para estandarizar los conceptos técnicos y científicos. «... el término *e-data* se refiere a datos que han sido inteligentemente modelados, depurados, y consolidados en un *data-warehouse*...» Es condición fundamental que estos *e-data* sean comprensibles y puedan usarse para los fines preconcebidos.

En la actualidad, el dato es el símbolo de una forma, suceso, entidad, etc.; su carácter también puede ser variable: numérico, alfabético, algorítmico,¹⁷ etc. El dato es el componente mínimo de la información; en ese sentido, de manera aislada o desordenada, en general, solo puede ser un componente. Por ejemplo, el dato *delito* es algo muy vago; no nos permite saber si se trata de un delito grave o de uno menor; no nos inclina a tener una idea completa o valoración adecuada en tanto no tenga otros componentes que le den valor a ese dato y nos produzcan información. No obstante, si a ese dato le añadimos otros aislados, como *asesinato, Juan C. y 2012, Guatemala*, entonces, al ordenarlos, asociarlos y contextualizarlos en el ámbito de la Criminología, me producen la siguiente información elemental: Juan C., en 2012 cometió el delito de asesinato en Guatemala. Esa unión y ordenamiento de datos hizo posible que yo consiguiera una información que me permitirá ubicarme y tener conocimiento sobre lo ocurrido.

Con este ejemplo puedo hacer un primer esquema de la vida de los datos:



De esta manera llego a la primera conclusión: los datos, de manera desordenada o inconexa, tienen poca relevancia para el entendimiento; solo hasta que se ordenan y procesan constituyen información; o sea, cuando se estructuran y por consiguiente contribuyen a la creación de conocimiento. No obstante, no toda estructura de datos constituye información. En el ejemplo anterior, los datos

¹⁷ Según la acepción 1 del DRAE, un algoritmo es el «Conjunto ordenado y finito de operaciones que permite hallar la solución de un problema.» (Edición digital. <http://buscon.rae.es/drae/srv/search?id=MPHdkliiFDXX21wlc025>).

delito, asesinato, Juan C., 2012, Guatemala, si no los estructuro adecuadamente (por ejemplo, dentro del contexto de la Criminología, o de la justicia, etc.) no producirán una información coherente.

Otra característica de los datos, para que produzcan información, es que sean veraces y coherentes. Si no poseo ese tipo de datos, no podré, por ejemplo, anticipar la lluvia. Fue lo que les pasó a los antiguos griegos y a otras civilizaciones que nos antecedieron: por no contar con sistemas de datos veraces y coherentes, para la explicación de los fenómenos naturales construyeron una mitología y religión que fueron muy imaginativas y fantásticas pero cuya verdad no era real sino una «verdad mágica»; en tal sentido la información producida por tales datos, de ninguna manera sería confiable para nosotros que poseemos tecnologías que nos permiten discernir de mejor manera sobre los datos. Fue necesaria la llegada, primero, de un pensamiento pre filosófico y luego de uno filosófico para tener explicaciones más coherentes con la realidad. Jostein Gaarder, en *El mundo de Sofía* nos explica esa transición: «Por filosofía entendemos una manera de pensar totalmente nueva que surgió en Grecia alrededor del año 600 antes de Cristo. Hasta entonces, habían sido las distintas religiones las que habían dado a la gente las respuestas a todas esas preguntas que se hacían. Estas explicaciones religiosas se transmitieron de generación en generación a través de los mitos. Un mito es un relato sobre dioses, un relato que pretende explicar el principio de la vida.»¹⁸

¹⁸ Gaarder, Jostein, *El mundo de Sofía*, Grupo Editorial Patria / Ediciones Siruela, México, 2014, Págs. 25-26.

Aunque hay investigadores que dotan de más elementos esenciales al dato, según Johan Galtun, en *Teoría y Métodos de la investigación social*, los elementos fundamentales de todo dato son:

1. Unidad de análisis
2. Variables
3. Valores¹⁹

La unidad de análisis estará constituida por el ámbito de lo que nos interesa averiguar, investigar o saber. En los tiempos del primitivo ser humano, cuando comenzó a tener razón y a ubicar los datos de manera ordenada y a deducir aspectos que debía tener en cuenta para su sobrevivencia, las unidades de análisis debieron constituirse las señales que anunciaban el suceso de determinados fenómenos naturales. Por ejemplo, la lluvia. Dentro de esta unidad de análisis a ese ser primitivo le interesaba saber o averiguar cuándo se produciría la lluvia; en ese sentido, los elementos que le darían certeza de que ese fenómeno ocurriría, serían: los truenos, los rayos que miraba en el cielo, el viento que corría más rápido, el oscurecimiento de las nubes, el refrescamiento del ambiente, etc.

En la actualidad, y dentro del ámbito de esta investigación, pongamos de ejemplo, como unidad de análisis, la Seguridad Ciudadana. Los elementos que podrán formar parte de este ámbito conceptual podrían ser: asesinatos, robos, asaltos, violencia contra la mujer, etc.

Las variables, que pueden ser dependientes o independientes, según incidan de manera directa o indirecta en la unidad de análisis, estarán constituidas por los

¹⁹ Citado en: <http://www.um.es/docencia/pguardio/documentos/Tec3.pdf>

diversos aspectos, características o particularidades que adoptan los distintos elementos de las unidades de análisis. Por ejemplo, dentro de la Seguridad Ciudadana, el elemento asesinato podría tener, entre muchas, las siguientes variables: dónde se producen con más frecuencia (V1), quiénes los ejecutan (V2), quiénes son las víctimas (V3), por qué se realizan (V4), etc. (VN). Y, para el ámbito de esta investigación, añadiré un elemento más dentro de las variables: las unidades de observación.

La valoración de los datos lo aportarían elementos como jerarquía, importancia, relevancia u otras asignaciones que el investigador, de acuerdo a los objetivos, le asigne a los elementos y variables de la unidad de análisis. Por ejemplo, dentro de la seguridad ciudadana, como unidad de análisis y del asesinato como elemento de esa unidad, podemos asignarle valores como impacto social, cuál es el perfil más frecuente del asesino, cuál es el perfil más frecuente de las víctimas, causas que más inciden en la consumación del asesinato, prevención de la criminalidad, etc.

1.2. Procesamiento de los datos

Ya vimos que el dato, como elemento aislado, tiene poca o nula importancia para crear información; en tal sentido, es fundamental que el dato se vincule con otros datos o elementos, de acuerdo con un fin u objetivo establecido previamente, para que sea útil; esa vinculación de un dato con otros elementos, o datos, constituye una etapa importante para la creación de la información y se le denomina procesamiento de datos.

La palabra «procesamiento» deriva de «proceso», cuya etimología es latina: *processus*. Las acepciones del vocablo «proceso» son, entre varias: desarrollo, tratamiento, marcha hacia adelante, avance, adelanto, progreso. «Un **proceso** es *cualquier* manipulación de datos, por lo general con el objetivo de producir información.»²⁰

De manera general, y en el contexto de esta investigación, el procesamiento de datos consiste en la selección de datos y la manera de ordenarlos, almacenarlos y evaluarlos, de acuerdo con un fin u objetivo previamente establecido; de esa manera, puedan ser de utilidad como fuente de consulta por usuarios que, con base en ellos, crearán información que, como resultado, sirva de fuente de análisis y base para la toma de decisiones.

Procesar los datos no es una actividad moderna; constituye una experiencia que arranca, prácticamente, desde los orígenes del ser humano. Lo que ha cambiado son los métodos, procedimientos y la complejidad de los soportes sobre los cuales se procesan. Los seres humanos primitivos debieron procesar los datos; debió ser fundamental para obtener información necesaria para su sobrevivencia.

En la medida en la cual el ser humano evolucionó, también cambió la manera de procesar los datos. En cada época debió evolucionar para adaptarse a los cambios que los requerimientos de la información era necesaria para mejorar su calidad de vida y, en especial, para proveerse de seguridad y certeza ante los peligros que le acechaban.

²⁰ Oz, Effy, *Op. Cit.*, Pág. 9.

La manera más elemental de procesar los datos fue memorizándolos; el soporte primario fue la memoria. Cada dato, por ejemplo el trueno, constituía un recurso mnemotécnico que al vincularlos con otros, como los rayos lumínicos que se observaban en el cielo, producían la información que la lluvia se acercaba. Luego, cuando la oralidad se estableció como medio de comunicación entre los seres humanos, los sonidos onomatopéyicos, que imitaban los de la naturaleza, constituyeron también datos para anunciar o predecir otros acontecimientos derivados de la interacción con la naturaleza. Después, cuando esos sonidos comenzaron a combinarse con otros simbólicos, pudieron procesarse datos de mayor complejidad hasta que, por medio de esos sonidos llegó el la lengua y el lenguaje.²¹ El cambio revolucionario se dio cuando los datos pudieron consignarse en soportes físicos, como las tabletas de cera, cerámica o madera. Toda esa evolución histórica, que no es el propósito de esta investigación evidenciar, nos llevó a experimentar los cambios más asombrosos, hasta que la era de la información nos hizo verlos como asunto cotidiano; ya no tenemos que esperar

²¹ La diferenciación entre lengua y lenguaje comenzó a hacerse conceptualmente a partir de lingüistas como Ferdinand de Saussure. En su obra póstuma, publicada en 1916 hace esta diferenciación: «... la lengua no se confunde con el lenguaje: la lengua no es más que una determinada parte del lenguaje, aunque esencial. Es a la vez un producto social de la facultad del lenguaje y un conjunto de convenciones necesarias adoptadas por el cuerpo social para permitir el ejercicio de esa facultad den los individuos. Tomado en su conjunto, el lenguaje es multiforme y heteróclito; a caballo en distintos dominios, a la vez físico, fisiológico y psíquico, pertenece además al dominio individual y al dominio social; no se deja clasificar en ninguna de las categorías de los hechos humanos, porque no se sabe cómo desembrollar su unidad.

«La lengua, por el contrario, es una totalidad en sí y un principio de clasificación. En cuanto le damos el primer lugar entre los hechos de lenguaje, introducimos un orden natural en un conjunto que se presta a ninguna otra clasificación.

«A este principio de clasificación se podría objetar que el ejercicio del lenguaje se apoya en una facultad que nos da la naturaleza, mientras que la lengua es cosa adquirida y convencional que debería quedar subordinada al instinto natural en lugar de anteponersele.» (Sussure, Ferdinand, *Curso de Lingüística General*, Editorial Losada, Argentina, 1945, Págs. 51-52).

siglos para experimentarlos. La computadora personal, por ejemplo, no tiene ni un cuarto de siglo de que fue accesible masivamente en Guatemala.

De la misma manera que la tecnología de soporte ha evolucionado, también lo ha hecho la manera de recolectar los datos, procesarlos y disponer de ellos. Ahora existen los sistemas de información; ya no se usan archivos monumentales, ni montañas de papeles sino que con *hardware* y *software* especializados, el trabajo se ha simplificado y facilitado la disposición y utilización de los datos. Veamos cuáles son los componentes de un sistema de información moderno, Según Effy Oz, en el libro ya citado *Administración de sistemas de información* (Pág. 16):

Datos	Hechos concretos, en su estado primario, que el sistema toma para producir información.
Hardware	Una computadora y su equipo periférico: dispositivos de entrada, salida y almacenamiento. El <i>hardware</i> también incluye equipo de comunicación de datos.
Software	Conjunto de instrucciones que indican a la computadora cómo obtener datos, procesarlos, desplegar información y almacenar datos e información.
Telecomunicaciones	Hardware y software que facilitan la transmisión y recepción rápida de texto, imágenes, sonido y animación en forma de datos electrónicos.
Personal	Profesionales y usuarios de los sistemas de información que analizan las necesidades de información de una organización, diseñan y construyen sistemas de información, escriben programas de computadoras, operan el <i>hardware</i> y

	mantiene el <i>software</i> .
Procedimientos	Reglas para lograr operaciones óptimas y seguras en el procesamiento de datos. Los procedimientos incluyen prioridades al ejecutar diferentes aplicaciones en la computadora, además de medidas de seguridad.

El ámbito de esta investigación es la información; de manera más específica, la información necesaria al Estado para cumplir los mandatos constitucionales que establecen: «Artículo 1º. Protección a la persona. El Estado de Guatemala se organiza para proteger a la persona y a la familia; su fin supremo es la realización del bien común.» Y, luego, el «Artículo 2º. Deberes del Estado. Es deber del Estado garantizarle a los habitantes de la República la vida, la libertad, la justicia, la seguridad, la paz y el desarrollo integral de la persona.» Y, además, «para que en forma integrada, sistematizada, eficiente y eficaz esté en capacidad de anticipar y dar respuesta efectiva a riesgos, amenazas y vulnerabilidades, a fin de estar preparado para prevenirlos, enfrentarlos y contrarrestarlos en observancia de la Constitución Política de la República, el respeto de los derechos humanos y el cumplimiento de los tratados internacionales ratificados por Guatemala.»²²

Concretando, la información sobre la cual trataré será la necesaria para dotar de la necesaria Seguridad Ciudadana, en el entendido de que esta es fundamental para los guatemaltecos, porque sin ella es muy difícil la realización humana plena, el desarrollo económico y social; en consecuencia, al no existir un clima de

²² Congreso de la República de Guatemala, *Ley Marco del Sistema Nacional de Seguridad*, 3er. Considerando.

seguridad, la armonía, la concordia y la aspiración al bien común, difícilmente podrá concretarse. Asimismo, si bien es fundamental la Seguridad Ciudadana, no es un estado que se consiga de manera fácil. Requiere de un proceso que de ninguna manera es aislado; está vinculado, prácticamente, con todos los órdenes de la vida humana. En ese sentido, su concreción depende de muchos factores; entre ellos, abordaré en esta investigación un elemento todavía novedoso de los componentes de la Inteligencia de Estado: la integración de las bases de datos de los Órganos de Seguridad del Estado. Pero, ¿por qué es necesaria la Inteligencia de Estado? En teoría, si uno se anticipa o prevé los sucesos que pueden acontecer, puede evitarlos. La misma sabiduría popular lo establece cuando esgrime el viejo refrán: «guerra avisada no mata soldados.» Prever, en este sentido, implica crear un ciclo de Inteligencia que, para el caso de Guatemala, se consigna en la *Ley Marco del Sistema Nacional de Seguridad* (Art. 2, inciso h) y consiste en el «conjunto de actividades realizado por las instituciones que conforman el Sistema Nacional de Inteligencia, que incluye: planificar, identificar información, recolectar, procesar, analizar, producir, distribuir y difundir información de manera oportuna, para la toma de decisiones al más alto nivel del Sistema Nacional de Seguridad.»

Quinientos años antes de nuestra era, Sun Tzu conocía la importancia de este aspecto y del énfasis que había que poner en la consecución de la información; así nos lo hace saber en el capítulo XIII, numeral 4: «Lo que se ha llamado “información previa” no puede obtenerse de los espíritus, ni de las

divinidades, ni de la analogía con acontecimientos pasados, ni de los cálculos. Es necesario obtenerlo de hombres que conozcan la situación del enemigo.»²³

1.3. Matrices para el procesamiento de datos

Para que los datos constituyan elementos para crear información, como ya se dijo, es preciso ordenarlos y sistematizarlos de acuerdo con un fin u objetivo específico. No podemos hacer uso adecuado de los datos si estos solo se almacenan de manera arbitraria y sin un orden establecido. En tal sentido, se precisa la creación de una matriz, o guía, que sirva para la recolección, ordenación y disposición de los datos para la posterior consulta, con base en las diversas unidades de análisis (UA) que se hayan establecido. No se puede confiar la recolección de los datos al criterio del recolector o recolectora, ya que los datos reunidos deben cumplir una función específica que no debe responder a la improvisación. En tales matrices se establecerá qué elementos son importantes y necesarios (variables) y qué valor (V) tienen para la creación de información; por tanto, deben consignarse de acuerdo con un criterio preestablecido.

A manera de recapitulación y ampliación sobre el dato, y previo a explicar y proponer el diseño de una matriz, debo decir que la constitución de un dato implica un universo de investigación construido dentro de una realidad; entonces, por medio de una elaboración conceptual, se registra en un soporte, ya sea de naturaleza física o simbólica, para que pueda ser expresado por medio de un lenguaje, también físico o simbólico. Para ilustrar este aspecto, a manera de

²³ Sun Tzu, *El arte de la guerra*, Colofón S. A., México, 2001, Pág. 118.

ejemplo, elaboraré el siguiente esquema de un universo de información. Como primer paso, los ordenaré en categorías y, a continuación, codificaré los elementos para que queden como referencias de la matriz de datos:

- Universo (U): Doctorado en Seguridad Estratégica

- Unidad de Análisis (UA):

1. Alumno 1 (UA1)

2. Alumno 2 (UA2)

3. Alumno 3 (UA3)

4. Alumno 4 (UA4)

- Variables (V):

Variable 1 (V1): Rendimiento académico (punteo)

Abierta

Variable 2 (V2): Entregó proyecto de tesis

1. Sí

2. No

Variable 3 (V3): ¿Comenzó su tesis?

1. Sí

2. No

Variable 4 (V4): ¿Qué aspecto de la seguridad abordó?

1. Político

2. Jurídico

3. Filosófico

4. Científico-tecnológico

Con estas referencias podré construir una matriz elemental, tipificada solo como ejemplo, utilizando un modelo entre muchos que pueden usarse, de acuerdo con las necesidades:

Universo de la información: Alumnos Doctorado en Seguridad Estratégica				
Unidad de Análisis	Variables			
	V1	V2	V3	V4
UA1	85	1	1	1
UA2	90	1	2	4
UA3	80	1	2	2
UA4	95	1	1	3
UAN				

Unidad de análisis: columna izquierda.

Variables: fila superior

Valores: celdas de la gráfica

La lectura que podemos hacer de esta gráfica, por ejemplo de la Unidad de Análisis 1 (Alumno 1), es la siguiente:

El alumno 1 obtuvo 85 puntos de calificación, entregó su proyecto de tesis, comenzó su tesis y la está trabajando sobre el aspecto jurídico.

1.4. El *data warehouse*

El proceso *data warehouse*,²⁴ es resultado de una tecnología relativamente reciente: el *warehousing*,²⁵ cuyo concepto surgió entre 1993 y 1994. Vino a

²⁴ En inglés, *Data warehouse*, significa, literalmente, depósito o almacén de datos.

²⁵ En inglés, *Data warehousing*, significa, literalmente, almacenamiento.

transformar, de manera gradual, los antiguos métodos de captación, recopilación, soportes y almacenamiento de datos. De manera general, un *data warehouse* es una terminal (o servidor) en la que confluyen los datos recolectados en estaciones, o fuentes (computadoras distintas al servidor) ubicadas en varios lugares. Siguiendo el esquema de Jil Diché,²⁶ en su libro *E-data*, el *data warehouse*, adaptado al propósito de esta investigación, tiene las siguientes características:

1. Es una plataforma, o computadora, generalmente aislada, aunque también pueden ser varias plataformas.

2. «Los datos en un *data warehouse* se usan para la toma de decisiones», o como elementos de consulta, análisis y creación de información para construir conocimiento acerca de un tópico específico.

3. Los *data warehouse* duplican información que reside en otros ámbitos de la entidad a que pertenecen; en este caso el SNS.

4. El *data warehouse*: «Es la combinación de hardware, software especializado y datos.»

Además, añadiría que:

5. Sea accesible; es decir que permita la navegación, un desempeño rápido, y que los contenidos sean comprensibles y ajustados a nuestros propósitos (que sean verdaderos, consistentes).

6. Que permita los cambios continuos sin que se pierdan los históricos; es decir, los que se han incorporado desde que se instaló el sistema.

²⁶ Diché, Jil, *E-data*, Prentice Hall, Buenos Aires, Argentina, 2001, pagina

7. Que sea un depósito seguro de la información para que esta quede resguardada y blindada contra los ataques externos o la pérdida de tal información.

8. Que este sistema pueda contar con un control de registro. ¿Qué quiero decir con esto? Que el sistema debe contar con un registro de quien maneja la información para verificar quién «accesó» a la información, y que deje huella de tal usuario. Ya sea que este haya consultado la información o haya hecho cambios en un expediente. De esta forma se tendrá el control del personal verificador de la información. En ese aspecto funcionará como un sistema similar al que utilizan los bancos cuando uno quiere solicitar su estado de cuenta. Para evitar que la misma gente del banco esté viendo datos personales de las cuentas bancarias a discreción, este sistema deja una marca o huella de quién fue el empleado del banco que «accesó» a ver tal información en la cuenta y, de esta manera, evitar futuros altercados o evasión de información.

1.5. Características de la información

Una primera definición de información, derivada del numeral 1.1, es que consiste en una serie de datos ordenados y clasificados que permiten el conocimiento sobre un asunto particular o general. En la información, el ordenamiento o clasificación de los datos debe tener una coherencia racional que permita su aprovechamiento para la toma de decisiones, la resolución de problemas y la contextualización adecuada, de acuerdo con los intereses u objetivos de quien los ordena o clasifica. Por ejemplo, los datos *delito, asesinato, Juan C., 2012,*

Guatemala, si los estructuro como datos en el contexto legal, me servirán de referencia para formarme una idea general del panorama siguiente: Juan C. enfrentará un juicio; en ese juicio puede ser condenado a muerte, aunque la sentencia no se ejecute en vista de que no está resuelto lo concerniente al recurso de gracia; además, que puede declararse confeso y evitar la condena a muerte; que deberá pagar una compensación a la familia de la persona asesinada, etc.

1.6. Clases de información

La información puede clasificarse de la manera más variada, de acuerdo con los objetivos, características, medios por los cuales se obtiene, etc. En el ámbito externo de la información suele clasificarse como pública, interna y privada. La información sobre la que trataré en esta investigación es pública porque se refiere a la población guatemalteca; no obstante, su manejo está restringido solo para las instituciones que conforman el SNS, pero como marca la ley, «sujeta a controles democráticos»²⁷; además, tal información está clasificada como información reservada, según el artículo 9, inciso 7 de la *Ley de Acceso a la Información Pública* y la establecida en el artículo 23 de la misma ley. Esa información también deberá manejarse dentro de un marco axiológico que deberá regir la conducta institucional; en el entendido de que el Estado y sus instituciones deben ser ejemplares en este aspecto que, en definitiva, será un factor que contribuirá a la credibilidad y confianza ciudadana en las instituciones adscritas al SNS. Al proceder de esa manera, también se estará contribuyendo a que la ciudadanía

²⁷ *Ley Marco del Sistema Nacional de Seguridad*, Capítulo III, artículo 3.

integre en su conducta valores que apunten hacia la elevación del nivel de vida de toda la población.

1.7. Teoría de la información

¿Una teoría de la información, planteada desde la matemática y no desde las ciencias sociales? Sí. Por poner un símil, es como conocer una obra literaria por medio de su versión cinematográfica. Es decir donde el lenguaje cambia; ordena, sintetiza y simplifica, de manera visual, la información contenida en la obra literaria. Así, por medio de la teoría de la información se simplifican los procesos de la información que se usaban antes; se evitan grandes almacenamientos de enormes volúmenes de papel, muebles, maquinaria, especialistas en ordenamiento, adecuación, etc. y, de todas maneras, la información se mostraba deficiente; también, tardada en obtenerla. Ahora para lograr su efectividad, se ha hecho posible que sea más eficaz y simple su proceso; es posible dotarla de las características siguientes: que sea precisa, exacta, íntegra y significativa. Con los insumos de la teoría de la información se ha logrado un máximo de compresión de los datos y un nivel máximo de transmisión de la información libre de errores.

El concepto de teoría de la información se ha consolidado por medio del uso, a pesar de que su nominación fue errática al no corresponder su nombre con su contenido. Esta asincronía se debe particularmente a que la teoría de la información, formulada inicialmente por Claude Shannon, no considera los aspectos semánticos y prácticos de la información; se concreta particularmente a cuantificar la información que se produce, transporta por un medio y se almacena,

pero no nos dice de qué información se trata. No obstante, la teoría de la información le dio un vuelco casi total a todo lo referente a la información y comunicación que ha repercutido de manera profunda en los hábitos personales, la manera de vivir, la interacción social y aun la manera de ver el mundo y sus circunstancias.

Antes, la preocupación fundamental fue la obtención de técnicas y tecnologías para la producción material: primero artesanal y después industrial. Ahora la inquietud primordial es descubrir y buscar mejores tecnologías para la producción, transmisión, almacenamiento y distribución de la información. Ya no es el conocimiento en sí lo que ocupa el pensamiento de manera primordial; ahora preocupa al ser humano con preeminencia la tecnología que sea capaz de obtener o mejorar la información y que haga más fluida la comunicación. En términos generales, la información ha mediatizado nuestras relaciones sociales; incluso los genes, que son los que le dan características propias a los seres humanos y son considerados como transmisores de información.

La información como elemento de la comunicación comenzó a gestarse a partir de lo oral y gestual; en ese sentido, tuvo una evolución que fue moldeándose gracias a la cultura de que fue dotándose el ser humano en su interacción con la naturaleza y en la convivencia misma con otros seres humanos; en esos contextos, comenzó a producir pensamiento abstracto, como la escritura y el lenguaje. Después apareció la imprenta. Luego dio un salto extraordinario cuando la electricidad pudo ser entendida, estudiada, manipulada y utilizada para beneficio de la humanidad. Con posterioridad se contó con un invento importante,

el telégrafo, que desarrolló uno de los elementos relevantes para la llamada teoría de la información: la compresión. Este aspecto es uno de los que más ha contribuido a los avances de la ciencia y modificar muchos aspectos de la vida cotidiana. Voy a poner un ejemplo sencillo que nos puede dar una idea de la magnitud del cambio que ha operado la capacidad de compresión de la información en nuestras circunstancias: una Biblioteca familiar compuesta por mil libros que caben físicamente en una librería de 0.25 mts. de ancho por 3 metros de largo, por 2.5 mts. de alto. Ahora es posible comprimir la información contenida en esos libros y almacenarlo en un disco compacto de 4.5 Gb. Solo eso es extraordinario. Es algo que hace unos veinte años no se podía hacer porque los discos compactos no se podían obtener en el mercado guatemalteco. Tan así nos ha permeado la llamada «teoría de la información» que nuestra era ha sido etiquetada como la «era de la información» y la sociedad como «sociedad de la información». Tan colosal transformación se ha logrado a partir de que Shannon propuso su teoría, hace menos de setenta años. Hay que tener en cuenta que una vez formulada, fue recibida con mucho escepticismo y fue blanco de abundantes críticas, hasta el día de hoy, pero es innegable la manera cómo influye en prácticamente todos nuestros actos y sin que seamos conscientes de tal realidad. «Shannon presentó y desarrolló una teoría que tenía como objetivo principal la definición matemática de todas aquellas magnitudes que intervienen en las situaciones en las que se produce un flujo o transmisión de información, y conseguir, a partir de esas definiciones, un cálculo de la cantidad de información

que puede ser transportada a través de un canal y la identificación, además, de las formas de maximizar la eficacia de ese proceso.»²⁸

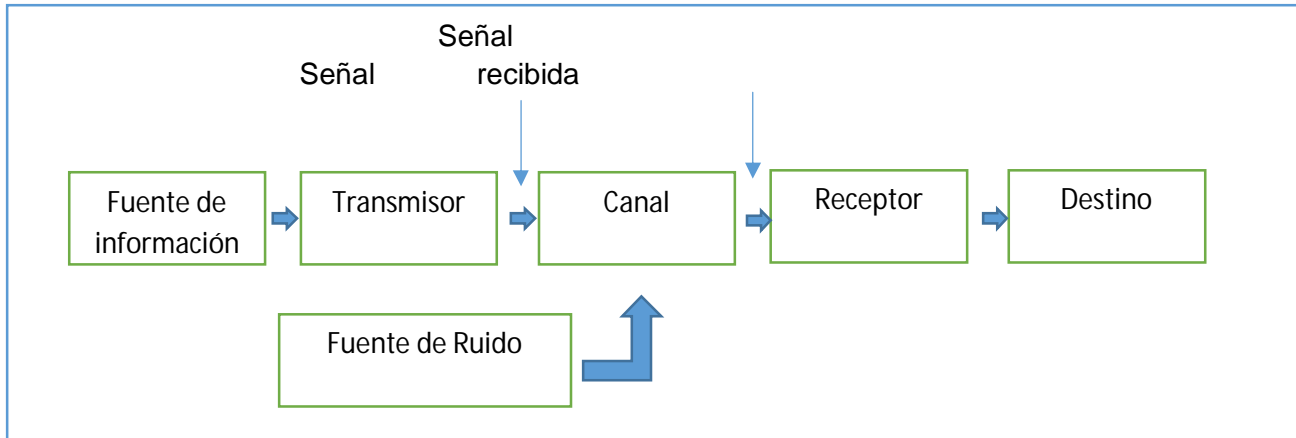
La teoría de la información transformó, de manera radical, el mundo de la información a partir de que Claude Shannon, en 1949, publicó su famoso libro *The Mathematical Theory of Communication*. Hasta ese momento, la información solo había sido objeto de estudio para los lingüistas, sociólogos, historiadores y humanistas en general. Muy pocos habían pensado que la comunicación y su componente la información, pudieran ser parte y objeto de estudio matemático. ¿Por qué? Porque solo habían sido objetos de estudio de las ciencias sociales y no de la ciencia matemática. La diferencia básica en los dos enfoques consiste en que las ciencias sociales se ocuparon de la esfera cultural; es decir, de lo no natural; y la matemática se ocupó de su aspecto natural. ¿Qué plantea Shannon en su libro? En primer lugar, aunque es complejo, suena sencillo: la información, sea cual fuere su formato, puede homogeneizarse por medio de un código binario;²⁹ o sea, toda información: sonido, imágenes, texto, etc. pueden procesarse con el código binario, factor fundamental del álgebra booleana³⁰ que, a la vez,

²⁸ Mario Pérez Gutiérrez, “Fundamentos básicos de la Teoría de la Información”, en: *Seminario de Teoría de la Comunicación II*, Universidad Surcolombiana, Pág. 3, obtenido en: <http://carmonje.wikispaces.com/file/view/02+Fundamentos+de+la+teor%C3%ADa+de+la+informaci%C3%B3n.pdf/360802260/02%20Fundamentos%20de%20la%20teor%C3%ADa%20de%20la%20informaci%C3%B3n.pdf>, Consultado el 27-2-2014, 17:00 horas.

²⁹ Código binario: está basado en el principio de interrupción y flujo de la electricidad; es decir, flujo e interrupción que son permitidas por el interruptor. Por ejemplo, cuando un bombillo se enciende, es señal que la electricidad está fluyendo a través de un circuito; cuando un foco se apaga, es señal que la electricidad dejó de fluir en el circuito. Estas dos operaciones se representan de la siguiente manera. Cuando el flujo está abierto, por el número 1. Cuando está cerrado, por el 0.

³⁰ El álgebra booleana, o álgebra de Boole, cuya designación deriva de su diseñador, el matemático inglés George Boole. Su diseño permite abstraer las operaciones algebraicas fundamentales en un sistema binario.

constituye el pilar del lenguaje digital. En segundo lugar expone la ruta que debe recorrer la información para convertirse en tal. Y lo muestra de manera gráfica en lo que después se dio en llamar el «modelo de Shannon»:



Modelo de Shannon³¹

Este modelo lo explica Warren Weaver, en el prólogo al libro de Shannon, de la siguiente manera: «La fuente de información selecciona a partir de un conjunto de posibles mensajes el mensaje deseado. (Como se verá, esta función es particularmente importante). El transmisor transforma el mensaje en una señal que es enviada por el canal de comunicación al receptor.

«El receptor hace las veces de un transmisor invertido que cambia la señal transmitida en un mensaje y pasa este mensaje a su destinatario. Cuando yo hablo con usted, mi cerebro es la fuente de información, el suyo el destinatario, mi sistema vocal es el transmisor, y su oído, con el octavo par de nervios craneanos, es el receptor.

«Infortunadamente, es característico del proceso de transmitir la señal que se agreguen a ésta ciertas cosas que no son proporcionadas deliberadamente por

³¹ Gráfica tomada de: Monsalve Ramírez, Alfonso, *Teoría de la Información y Comunicación Social*, Ediciones Abya-Yala, Ecuador, 2003, Pág. 24.

la fuente de información. Estos aditamentos indeseados pueden ser distorsiones de sonido (en telefonía, por ejemplo), o estáticos (en radiotelefonía), o distorsiones en la sombra o en el sombreado de una imagen (televisión), o errores de transmisión (telegrafía o facsímil). Todos esos cambios en la señal pueden ser llamados ruidos.»³² De manera práctica, este proceso de comunicación de información, puede ser explicado por medio de la conversación telefónica entre dos estudiantes (Estudiante 1 y Estudiante 2) del Doctorado en Seguridad Estratégica:

Alumno	Conversación	Elemento del modelo de Shannon
Alumno 1:	Estoy en la biblioteca de la Universidad; terminé mi parte de la tarea y te la acabo de enviar a tu correo electrónico.	<ul style="list-style-type: none"> • El alumno 1 constituye la fuente de información. • Lo que le dice constituye el mensaje. • El teléfono es el transmisor del mensaje que lo convierte en señal eléctrica. • El cableado telefónico servirá de canal de comunicación para la señal eléctrica que produjo el teléfono. • La señal es recibida en el teléfono (receptor) del alumno 2.

³² Ibídem, Págs. 23-24.

		<ul style="list-style-type: none"> • El alumno 2, entonces, puede considerarse el Destino.
Alumno 2:	No te escucho bien; se oye una interferencia de otra conversación telefónica que no me permite entenderte bien. Cortemos y luego me llámás.	<ul style="list-style-type: none"> • Esa interferencia a que alude el alumno 2, dificulta la comprensión del mensaje del alumno 1. Es lo que Shannon llama fuente de ruido.

La teoría de la información, como todo aspecto relacionado con la filosofía o la ciencia, no surgió de manera espontánea; fue producto de un aprendizaje previo, de una «ordenación precientífica». Por ejemplo, para que la filosofía se concretara hubo que transcurrir primero, en el pensamiento de los humanos, un período mitológico en el cual a lo inexplicable racionalmente se le atribuían «razones» mágicas que luego se traducían en mitos que se transmitían de boca en boca y eran memorizados colectivamente teniéndoseles por verdades inmutables que no podían transgredirse so pena de recibir un castigo divino. Uno de estos mitos, que ponen de manifiesto el castigo divino, es el de Prometeo que engañó a Zeus: «Una primera vez, en Mecone, durante un sacrificio solemne, había hecho dos partes de un buey: en un lado puso la carne y las entrañas, recubriéndolas con el vientre del animal; en otro puso los huesos mondos, cubriéndolos con grasa blanca. Luego dijo a Zeus que eligiese su parte; el resto quedaría para los hombres. Zeus escogió la grasa blanca, y, al descubrir que sólo contenía huesos, sintió un profundo rencor hacia Prometeo y los mortales, favorecidos por aquella

astucia. Para castigarlos decidió no volverles a enviar fuego. Entonces Prometeo acudió en su auxilio por segunda vez; robó semillas de fuego en “la rueda del Sol” y las llevó a la tierra ocultas en un tallo de férula. (...) Zeus castigó a los mortales y a su bienhechor. Contra los primeros ideó enviar un ser modelado ex profeso, Pandora.³³ En cuanto a Prometeo, lo encadenó con cables de acero en el Cáucaso, enviando un águila, nacida de Equidna y de Tifón, que le devoraba el hígado, el cual se regeneraba constantemente.»³⁴ Luego vino el pensamiento pre filosófico que comenzó a plantearse, con herramientas rudimentarias del pensamiento, respuestas a sus preguntas sobre el entorno que lo circundaban. Entonces, y con las herramientas intelectuales que esos dos procesos habían conseguido, advino la filosofía, a cuya vanguardia estuvieron Sócrates, Platón y Aristóteles. Fue en ese momento cuando los humanos comenzaron a preguntarse por su situación como seres dentro de ese entorno que los pre filósofos o presocráticos, como se ha dado en llamarles: habían comenzado a indagar. «Decimos que tuvo lugar una evolución de una manera de pensar mítica a un razonamiento basado en la experiencia y la razón. El objetivo de los primeros

³³ «En un mito hesiódico, Pandora es la primera mujer. Fue creada por Hefesto y Atenea, con la ayuda de todos los dioses y por mandato de Zeus. Cada uno le confirió una cualidad, y, así, recibió la belleza, la gracia, la habilidad manual, la persuasión, etc.; pero Hermes puso en su corazón la mentira y la falacia. (...) Zeus la envió a Epimeteo, el cual, olvidando el consejo de su hermano de no admitir ningún presente de Zeus, se dejó seducir por su belleza y la hizo su esposa. Ahora bien, existía una jarra —Hesíodo no dice en qué consistía— que contenía todos los males. Estaba cerrada con una tapadera que impedía que su contenido escapase. No bien hubo llegado a la Tierra, Pandora, picada por la curiosidad, abrió la vasija, y todos los males se esparcieron por el género humano.» (Grimal, Pierre, *Diccionario de Mitología Griega y Romana*, Ediciones Paidós, España, 1994, Pág. 405).

³⁴ Grimal, Pierre, *Diccionario de Mitología Griega y Romana*, Ediciones Paidós, España, 1994, Pág. 455.

filósofos era buscar *explicaciones naturales* a los procesos de la naturaleza.»³⁵ Igual pasó con la ciencia, que tuvo una evolución muy similar y de la mano con el nacimiento de la filosofía: el conocimiento precientífico. Al principio también, sin un método adecuado (característica fundamental del proceso científico) los humanos se encontraban en un mundo de explicaciones mágicas a lo ocurrido en su entorno; no obstante, basados en la observación comenzaron a obtener respuestas y explicaciones más coherentes de lo que ocurría en su entorno; es decir, comenzaron a explorar fuera de lo mítico y lo sagrado. Según cuenta Carl Sagan, el nacimiento de la ciencia se dio cuando, en el siglo VI antes de nuestra era, se comprobó que el universo era cognoscible a partir de cierto orden y ciertas regularidades en la naturaleza que permitían descubrir sus secretos y deducir qué es predecible.³⁶ Así también, la teoría de la información estuvo antecedida por procesos pre-científicos como la clave Morse, el sistema Braille, etc., en lo que respecta al proceso de comprensión de la información.

En el capítulo III, ampliaré más este proceso de manera técnica. Lo que me propuse en este capítulo fue solamente esbozar, de manera descriptiva, los conceptos fundamentales que dirigirán esta investigación. Por otra parte, mi investigación no estará enfocada en los procesos sociales de la comunicación e información sino en la aplicación de la ciencia matemática (codificación de los datos y la información, medición de la información, compresión de la información, decodificación e interpretación, probabilidad, estadística, etc.) a la consecución de

³⁵ Gaarder, Jostein, *Op. Cit.* Pág. 32.

³⁶ Sagan, Carl, *El origen de la ciencia*, documental, en: <https://www.youtube.com/watch?v=fugAnWE5Ry0>

los insumos necesarios que aseguren una seguridad estratégica; en consecuencia, los principios filosóficos y políticos de la investigación están consignados en la *Constitución Política de la República de Guatemala*, en la *Ley Marco del Sistema Nacional de Seguridad* y otros instrumentos legales vigentes en la legislación guatemalteca; también, en los instrumentos legales internacionales de los que Guatemala es signataria. De manera más específica, abordaré la información como un asunto fundamental para la garantía de la Seguridad de la Nación³⁷ en el marco de la Seguridad Democrática³⁸ que será posible, en buena medida, al producir Inteligencia de Estado,³⁹ a sabiendas de que en la medida que ese objetivo se concrete, se creará un clima más adecuado para el desarrollo y la realización humana de los habitantes guatemaltecos; esa será la vértebra epistemológica de esta investigación. Derivado de lo anterior, estará enfocada a

³⁷ «**Seguridad de la Nación:** La Seguridad de la Nación incluye el conjunto de principios, políticas, objetivos, estrategias, procedimientos, organismos, funciones y responsabilidades de los componentes del Estado en materia de seguridad, que garantizan su independencia, soberanía e integridad, y los derechos fundamentales de la población establecidos en la Constitución Política de la República de Guatemala, consolidando la paz, el desarrollo, la justicia y el respeto de los derechos humanos.» (*Ley Marco del Sistema Nacional de Seguridad*, Capítulo II, Artículo 2, inciso a).

³⁸ «**Seguridad Democrática.** La Seguridad Democrática es la acción del Estado que garantiza el respeto, promoción y tutela de la seguridad, al mismo tiempo que el pleno ejercicio de los derechos humanos, mediante la creación de condiciones que le permita a la persona su desarrollo personal, familiar y social en paz, libertad y democracia, conforme a lo establecido.» (*Ley Marco del Sistema Nacional de Seguridad*, Capítulo II, Artículo 2, inciso b).

³⁹ «**Inteligencia de Estado.** La Inteligencia de Estado es la capacidad institucional del Estado, conforme ley, para disponer de información oportuna, veraz y pertinente para la toma de decisiones, con el fin de garantizar la seguridad de la Nación a través del cumplimiento del ciclo de Inteligencia. [«El ciclo de Inteligencia es el conjunto de actividades realizado por las instituciones que conforman el Sistema Nacional de Inteligencia, que incluye: planificar, identificar información, recolectar, procesar, analizar, producir, distribuir y difundir información de manera oportuna, para la toma de decisiones al más alto nivel del Sistema Nacional de Seguridad.» (*Ley Marco del Sistema Nacional de Seguridad*, Capítulo II, Artículo 2, inciso h)].

«Constituye el conjunto de competencias y procedimientos especiales asignados, mediante ley, exclusivamente a instituciones públicas especializadas, para que realicen en ámbitos diferenciados, la obtención de información, su análisis y su transformación en un producto útil para la toma de decisiones.» (*Ley Marco del Sistema Nacional de Seguridad*, Capítulo VI, Artículo 23).

demostrar que la integración de base de datos de los Órganos de Seguridad del Estado es fundamental para prevenir actos delincuenciales y fortalecer la cultura de denuncia.

Haré un recorrido (análisis de los distintos organismos estatales) por medio de las formas de recolectar la información, en torno a las denuncias que se hacían y se hacen en las distintas instituciones del Estado que, en el curso de la historia reciente, se han encargado de esta tarea. Su enfoque estará dirigido a demostrar que aun se utilizan maneras anacrónicas de recolectar la información en algunas instituciones estatales y que tal proceder incide en la baja efectividad de las denuncias para prevenir, disuadir y combatir al crimen; por tanto, en la consecuente falta de confianza de la población en tales instituciones y, por tal razón, en el desinterés en adoptar una cultura de denuncia. En seguida me concentraré en proponer un sistema por medio del cual se pueda integrar toda la información que se reciba en tales instituciones y la manera de administrarlas.

Capítulo II

1. Inteligencia de Estado

Hay diversas definiciones para Inteligencia de Estado; en el curso de esta investigación me referiré a algunas de ellas, de manera referencial; sin embargo, para los fines de esta investigación, que se da en el contexto guatemalteco, me apoyaré sobre todo en esta: «Inteligencia de Estado es la capacidad institucional del Estado, conforme ley, para disponer de información oportuna, veraz y pertinente para la toma de decisiones, con el fin de garantizar la seguridad de la Nación a través del cumplimiento del ciclo de Inteligencia.

»Constituye el conjunto de competencias y procedimientos especiales asignados, mediante ley, exclusivamente a instituciones públicas especializadas, para que realicen en ámbitos diferenciados, la obtención de información, su análisis y su transformación en un producto útil para la toma de decisiones.»⁴⁰

En cierto sentido, la Inteligencia de Estado es hija de la guerra. Surgió en la Antigüedad como una necesidad de los gobernantes de saber todo lo relativo a su enemigo, real o potencial, para poder vencerlo en la guerra, o anticiparse a sus amenazas dentro o fuera de su Estado. Sus formas de practicarla también han sido diversas y han respondido, entre muchas causas, a necesidades puramente prácticas, modelos basados en ideologías, o coyunturas que van desde las creadas artificialmente hasta las inesperadas y de corte puramente fortuito.

⁴⁰ Congreso de la República de Guatemala, *Ley Marco del Sistema Nacional de Seguridad*, Guatemala (Art. 23), 2008.

Lo que modernamente llamamos Inteligencia Estratégica, según Sun Tzu, aproximadamente 500 años antes de Cristo (a. de C.), en lo concerniente a la guerra, lo llamaba información previa: «Pues si el príncipe esclarecido y el general competente derrotan al enemigo cada vez que pasan a la acción, si sus hazañas se salen fuera de lo común, es gracias a la información previa.»⁴¹ Añadía: «Lo que se ha llamado “información previa” no puede obtenerse de los espíritus, ni de las divinidades, ni de la analogía con acontecimientos pasados, ni de los cálculos. Es necesario obtenerlo de hombres que conozcan la situación del enemigo.»⁴²

En la medida en la que se establecían los reinos y los imperios, la Inteligencia de Estado fue cada vez más necesaria y los métodos de Inteligencia se fueron sofisticando. Los romanos aprendieron no solo a recolectar datos referenciales sobre el enemigo sino, también, a conocerlo a fondo para entender cómo actuaría. De la simple recolección o transmisión de la información se pasó al cifrado. «Se atribuye a Julio César haber inventado el primer código cifrado para transmitir informaciones secretas.»⁴³ Eso ocurrió en la segunda mitad del siglo I a. de C.

Julio César también sabía la importancia estratégica de contar con información fresca, fidedigna y oportuna para analizarla y actuar con ventaja y certeza. Eso le fue de mucha utilidad para salir vencedor en la Guerra de las

⁴¹ Sun Tzu, *El arte de la guerra*, Colofón S. A., México, 2001, Pág. 118.

⁴² *Íbid.*

⁴³ En: “Inteligencia”, *Enciclopedia de la Política*, tomado de: <http://www.encyclopediadelapolitica.org/Default.aspx?i&por=i&idind=822&termino>

Galias.⁴⁴ Un ejemplo de esa habilidad se manifestó cuando en esa guerra, se enfrentó al jefe de los germánicos, Ariovisto. Este dirigente poseía un ejército muy bien entrenado, valiente y cruel; se acercaba a la ciudad de Beçanson para establecer allí su base de operaciones, a unos 30 kilómetros de donde estaba asentado el ejército de Julio César. Pero hubo un dato muy importante que le proporcionó enorme ventaja a Julio César. A través de sus informantes, se enteró, poco antes de marchar contra el ejército de Ariovisto, de algo que era común entre los ejércitos de la Antigüedad. Estos, cuando marchaban a la guerra solían llevar con ellos a sacerdotes, adivinos y otros personajes, como mujeres videntes; se suponía que podían establecer contacto con los dioses y averiguar sus designios por medio de los más variados rituales. Entonces, las mujeres videntes al escuchar la pregunta de Ariovisto sobre si aconsejaban los dioses ir a la batalla y ganarla, practicaron un ritual para, según sus creencias, ponerse en contacto con los dioses; como resultado de esa práctica, establecieron que Ariovisto no debía enfrentarse a Julio César antes que la luna nueva apareciera. Y, claro, Ariovisto tenía la convicción de que debía obedecer ese designio. Julio César se enteró; con esa información sabía que tenía una enorme ventaja psicológica sobre el ejército de Ariovisto si atacaba antes de la luna nueva. Y así lo hizo. Los bárbaros germánicos estaban fortificados y era preciso que Julio César los provocara para hacerlos salir de su fortificación y establecer el combate. Entonces, al ejército de

⁴⁴ Se llama Guerra de las Galias a las batallas libradas entre Julio César (procónsul romano) y los germanos por la conquista del territorio de Las Galias. Estos sucesos ocurrieron entre los años 58 y 51 a. de C. El mismo Julio César, respecto a estos enfrentamientos escribió el libro *Comentarios a la Guerra de las Galias*.

Ariovisto no le quedó más remedio que combatir a sabiendas que, según sus dioses, iban a perder la batalla, como en efecto sucedió.

Siglos después, en el XIII, Gengis Kan, la analfabeta que después llegó a ser un gran estratega, interrogó al viajero Marco Polo para obtener información sobre lo que pasaba fuera de los lindes de su imperio y sobre cómo actuaban, pensaban y vivían las personas en los territorios que Marco Polo conocía. Y guardaba esa información para utilizarla en el desarrollo de sus planes políticos; en preparar estrategias para que el comercio fluyera de Oriente a Occidente de manera más segura. Gengis Kan conocía bien la importancia de la información y de que, para su tiempo, fuera lo más fluida; por eso tenía un servicio de postas, que proveía a sus mensajeros de alimentación, caballos y relevos para que solo tardaran lo indispensable en llegar al destino especificado. Era un servicio muy eficaz, por medio del cual enviaba y recibía información sobre lo que pasaba en todos los rincones de su imperio y transmitía sus órdenes. Eso le proporcionó la suficiente estabilidad para gobernar. Consciente de la importancia de una información fidedigna, antes de emprender una campaña guerrera contra un pueblo, enviaba emisarios, comerciantes o personas encubiertas para que colectaran información sobre la población, el comercio, los ejércitos (número de soldados, fortalezas, debilidades, etc.), el territorio y otras características que le dieran una idea global sobre el enemigo. Solo cuando tenía la información suficiente se lanzaba contra él. Un hecho, entre muchos, ilustra perfectamente este aspecto de recabar anticipadamente información sobre su enemigo. Cuando Gengis Kan ya se había consolidado como un guerrero eficaz, tuvo la idea de unificar a todas las tribus

nómadas en una sola; su antiguo amigo Yamuka se le opuso. Entonces, Gengis Kan averiguó todo sobre el ejército de Yamuka y, sabiendo que era muy superior a su ejército, la noche antes de la batalla planeó algo que él sabía le daría la victoria. Gengis Khan ordenó a sus soldados que, acampados en la estepa, en lugar de encender una fogata cada soldado, encendieran cinco cada uno. Cuando el ejército de Yamuka vio la cantidad de fogatas que el ejército de Gengis Khan tenía, se horrorizó al pensar en la superioridad del ejército enemigo y, esa misma noche, muchos desertaron. Al día siguiente los soldados de Yamuka, psicológicamente atormentados, sucumbieron ante el ejército inferior numéricamente de Gengis Khan.

Otro paso importante en el proceso de la concepción de Inteligencia fue la de ordenar los datos y disponer de personas especializadas en almacenarlos para que fuera posible consultarlos cuando se requiriese. «El primer servicio de Inteligencia de estructura moderna lo creó Napoleón, con cuadros permanentes, jerarquías y elementos especializados.»⁴⁵ Durante la época napoleónica, se esbozó el servicio de Inteligencia; a partir de ese momento histórico, la Inteligencia de Estado transformó la manera de manejar la información; el ciclo de Inteligencia (del que hablaré en el apartado siguiente) para administrar este recurso estuvo, sobre todo, concentrado en manos de Joseph Fouché. Este personaje, a pesar de su veleidad ideológica y del odio que Napoleón llegó a desarrollar hacia él, fue indispensable para su gobierno. Fouché tuvo el talento para establecer la más extensa red de colectores de información; para ordenarla, clasificarla, analizarla y

⁴⁵ «Inteligencia», *Op.Cit.*

presentarle informes diarios, todas las noches de todos los días, excepto los domingos, a Napoleón. A pesar de haber destituido Napoleón a Fouché tres veces, siempre lo volvió a llamar porque la información que le proporcionaba era, también, indispensable para la estabilidad de su régimen. De esa manera Fouché se volvió, prácticamente, indispensable. Por eso, Napoleón se dio cuenta tardíamente del error de haber concentrado casi toda la administración de la información, prácticamente, solo en Fouché pero el poder imperial, según Napoleón, así lo exigía. Esa manera de pensar fue heredada por casi todos los regímenes de casi todos los países hasta bien entrado el siglo XX; hasta que la democracia, después de la Segunda Guerra Mundial, sobre todo por medio de organismos internacionales como la ONU, se convirtió casi en una exigencia para los países de Occidente; eso mismo obligó a los gobiernos a estructurar sus sistemas de Inteligencia teniendo como referente las nuevas formas de convivencia social.

Sin un efectivo servicio de Inteligencia, la Segunda Guerra Mundial no la habrían ganado los Aliados. El desembarco en Normandía es un claro ejemplo de la importancia que la Inteligencia Estratégica tenía para entonces y de la necesidad de asegurar que el enemigo no se enterase de los planes ni de la información ajena. Ese fue una de las claves para la derrota alemana.

Los Aliados lograron decodificar los mensajes cifrados; de esa manera, tuvieron una idea más precisa del actuar del ejército alemán y de sus planes. Entonces, basados en esa información, los Aliados estuvieron en una posición de ventaja estratégica que la utilizaron para encubrir sus planes. ¿Qué hicieron?

Resolvieron la invasión a Europa haciéndoles creer a los alemanes que el desembarco ocurriría en un lugar distinto al verdadero. Había tres posibles locaciones para el desembarco: el Paso de Calais, la península de Cherburgo, o las playas de Normandía. Los Aliados les hicieron creer a los alemanes que el desembarco ocurriría en el Paso de Calais. Para eso montaron en dicho lugar un ejército fantasma; es decir, por la noche instalaron tanques, aviones y camiones a lo largo del Paso de Calais... solo que eran de plástico inflable. Para darles veracidad y que las fotografías aéreas no delataran el engaño, hicieron que hombres en patines simularan las huellas de esos artefactos inflables; además, transmitieron informaciones falsas sobre los movimientos que iban a realizar: número de tropas, material bélico, etc. Los Aliados sabían que las decisiones se concentraban en Hitler y no las delegaba en ninguno de sus subalternos; en consecuencia, sus comandantes nada podían hacer sin la venia de él; así que los Aliados tenían otra ventaja a su favor porque las decisiones siempre tardarían un poco en llegar a la zona de operaciones; en ese sentido, el tiempo fue un factor fundamental que estos aprovecharon y desembarcaron, el 6 de junio de 1944, en donde menos lo esperaban los alemanes: Normandía.

Los excesos cometidos durante las guerras, sobre todo en la Segunda Guerra Mundial, hicieron imperiosa la necesidad de los Estados de contar con un sistema de información que fuera capaz de propiciar ideas anticipadas sobre cómo enfrentar las amenazas internas y, especialmente, externas que se cernían sobre ellos. De esa manera, gracias a que las guerras también propiciaron el surgimiento de nuevas tecnologías militares, después se adaptaron al uso ciudadano; también

la Inteligencia de Estado, valiéndose del método científico, comenzó a conformarse y a convertirse en soporte teleológico del Estado.

No obstante lo anterior, cuando más se desarrollaron los servicios de información e Inteligencia de Estado fue a partir de la llamada Guerra Fría (o, Tercera Guerra, como la llamó el conde Alexandre de Marenches), «que no es más que la confrontación militar, económica, política, diplomática y psicológica, planetaria entre los Estados Unidos y la Unión Soviética, dos modelos económicos y políticos antagónicos —capitalismo y socialismo— en escenarios externos a ambas potencias.»⁴⁶ El mundo, en la práctica, se partió en dos: los capitalistas y los comunistas; muy pocos quedaron en medio. El capitalismo estaba representado por Estados Unidos y el comunismo por la Unión Soviética. En ese contexto, la violencia de la guerra no se practicó en campos específicos de batalla; dejó de tener un ámbito puramente geográfico y se extendió al campo social, incluso al ámbito personal. Las formas de violencia se volvieron más sutiles, pero los avances tecnológicos han logrado que los objetivos de dominación y obtención de poder sigan prevaleciendo en favor de una minoría y en detrimento de la mayoría. En resumen, la guerra ya no se planteó solo como el enfrentamiento de dos ejércitos en un campo de batalla sino que también se hizo inmaterial; es decir la lucha abarcó, prácticamente, todos los ámbitos de la vida social, material y mental.

⁴⁶ Pérez García, Juan Francisco, *La Inteligencia de Estado abre y cierra el siglo XX en Guatemala: Análisis de las formas y el sistema de Inteligencia durante los regímenes de Manuel Estrada Cabrera (1898-1920) y Militar Contrainsurgente (1960-1996)*, Universidad de San Carlos de Guatemala, Guatemala, 2007, Pág. 9.

En Guatemala también cambió la violencia después de la firma de los *Acuerdos de Paz* sin que se hubiesen resuelto las causas estructurales que dieron origen a la guerra.

A Guatemala, por la cercanía con Estados Unidos, y en su calidad de Estado débil, no le quedó más que adaptarse a estar bajo su influencia y a adoptar los métodos, incluso para su seguridad interna, que tal país le impuso; incluyendo la Inteligencia de Estado. De hecho, antes de la Segunda Guerra Mundial, Estados Unidos había comenzado a hacer sentir de manera inequívoca su influencia y presencia en Guatemala; la consolidación de esa influencia comenzó a ser muy visible a partir del gobierno de Manuel Estrada Cabrera; se afianzó con los gobiernos posteriores y se evidenció de manera total con Jorge Ubico. A partir de allí se hizo evidente la intervención estadounidense sobre nuestro país; a tal punto que, bajo el argumento de la amenaza soviética, cuyo régimen era comunista, Estados Unidos dispuso que, por esa razón, todo lo que oliera a comunismo debería cortarse de tajo pues constituía una amenaza para su seguridad; en consecuencia, los países latinoamericanos también debían considerar el comunismo como una amenaza para su seguridad interior. La suposición de que los países latinoamericanos deberían someterse a los intereses estadounidenses no se disimuló: «Pocos días después de su llegada a Guatemala a finales de 1953, Peurifoy [embajador de Estados Unidos en Guatemala] sermoneó al presidente Arbenz por su tolerancia hacia los comunistas, para después advertirle que las relaciones entre Estados Unidos y Guatemala seguirían tirantes mientras un solo comunista permaneciera en la nómina pública. Después de esto, Peurifoy

y el presidente nunca se hablaron...»⁴⁷ En ese marco los estadounidenses montaron la operación PBSUCCESS para derrocar al gobierno de Jacobo Árbenz Guzmán e imponer un gobierno que no dudara en someter la soberanía guatemalteca al albedrío estadounidense. Pero de esto hablaremos más adelante.

Antes de proseguir con el repaso sobre cómo la Inteligencia de Estado evolucionó a través del tiempo veamos ahora, de manera epistemológica, sus características. Al principio de este capítulo quedó definida la primera instancia epistemológica al respondernos qué es la Inteligencia de Estado según la *Ley Marco del Sistema Nacional de Seguridad*.

Ahora me enfocaré en responder una segunda cuestión epistemológica: ¿Cómo es la Inteligencia de Estado? *Stricto sensu*, la Inteligencia de Estado debe ser un instrumento para su mejor desempeño; que le permita cumplir de manera primordial su función teleológica, contenida en la *Constitución Política de la República de Guatemala* (Art. 1º): «El Estado de Guatemala se organiza para proteger a la persona y a la familia; su fin supremo es la realización del bien común.» En tal vía, la Inteligencia de Estado debe permitirle al Estado, en función de la ciudadanía, su defensa, estabilidad y sobrevivencia; la Inteligencia de Estado debe dotar al Estado de «la facultad de anticiparse a los hechos, bien para administrar el cambio como gestor o actor significativo del mismo, actuando en forma proactiva, o bien para adoptar y adaptarse al mismo, actuando en forma preventiva u oportunamente reactiva.»⁴⁸

⁴⁷ Schlesinger, Stephen y Kinzer, Stephen, *Fruta Amarga / La CIA en Guatemala*, Siglo XXI Editores, México, 1987, Pág. 27

⁴⁸ Cáceres G., *Op. Cit.*

¿Para qué existe la Inteligencia de Estado? Para proveer de conocimiento al Estado que le asegure su defensa, estabilidad y sobrevivencia. Como el Estado constituye la representación de una sociedad, una de sus condiciones primarias es el poder. El poder, sin su base que es el conocimiento, sencillamente colapsaría. Ese conocimiento necesario al Estado para desarrollar sus funciones lo produce la Inteligencia de Estado.

¿Por qué es inherente al Estado la Inteligencia de Estado? Porque si la Inteligencia de Estado le permite al Estado su defensa y estabilidad, entonces debemos considerarla como una función indispensable para su sobrevivencia. De otra manera, al no contar el Estado con esa función que le permite anticiparse a las amenazas que se ciernen contra él, entonces, sencillamente desaparecería o se convertiría en algo distinto a un Estado. Es como que a alguien, a quien le es fundamental determinada medicina para su sobrevivencia, se le dejara de proveer; sencillamente, moriría. Por eso, en la actualidad, es imposible que un Estado pueda prescindir de una Inteligencia de Estado capaz de proveerlo de «información e Inteligencia de amenazas, riesgos y vulnerabilidad internas y externas.»⁴⁹

La Inteligencia de Estado debe satisfacer las necesidades de información del Estado de la manera más eficaz. «Por tanto, se hace necesario implementar los mecanismos adecuados para manejar y dar forma a la información. En este

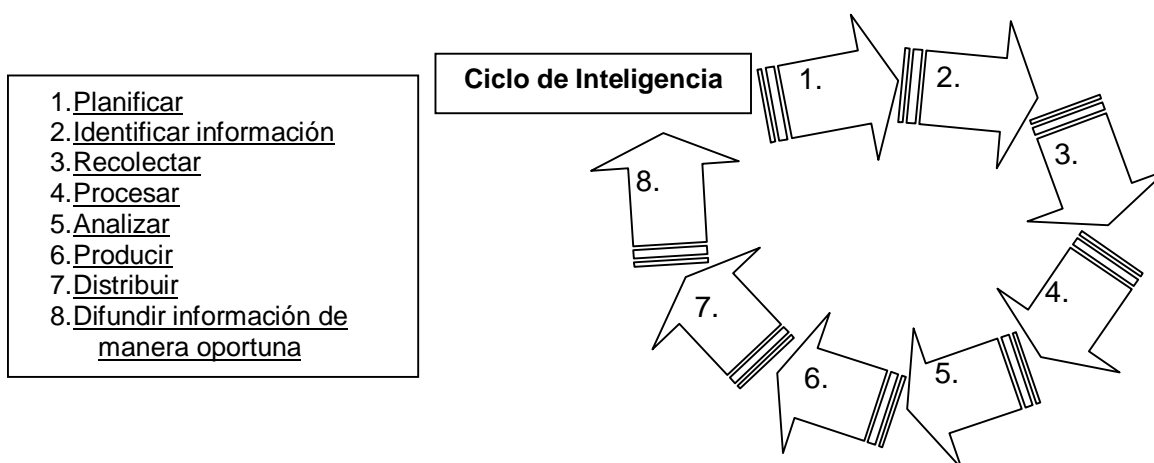
⁴⁹ *Ley Marco del Sistema Nacional de Seguridad*, Capítulo V, Artículo 21.

escenario irrumpe la disciplina de la epistemología como una herramienta para “amueblar nuestra cabeza” y enseñarnos a pensar.»⁵⁰

1.1. Ciclo de Inteligencia

De la misma manera que en el numeral anterior, para esta investigación el Ciclo de Inteligencia tendrá como referente principal lo consignado en la *Ley Marco del Sistema Nacional de Seguridad* (Artículo 2, inciso h): «El Ciclo de Inteligencia es el conjunto de actividades realizado por las instituciones que conforman el Sistema Nacional de Inteligencia, que incluye: planificar, identificar información, recolectar, procesar, analizar, producir, distribuir y difundir información de manera oportuna, para la toma de decisiones al más alto nivel del Sistema Nacional de Seguridad.»

En la Inteligencia moderna, uno de sus elementos fundamentales es el análisis. «El análisis de Inteligencia proporciona a los funcionarios civiles y militares, tomadores de decisiones políticas, información directamente relacionada con los temas que enfrentan y con las decisiones que tienen que tomar.»⁵¹



⁵⁰ Somiedo, Juan Pablo, en: *Inteligencia y Seguridad*, Revista de análisis y prospectiva No. 12, Editorial Foreword, España, 2012, Pág. 243.

⁵¹ ESISEN, *Análisis de Inteligencia*, Lecturas Básicas de Inteligencia 2, CISEN, México, 2009, Pág. 17.

2. Los elementos de la Inteligencia en Guatemala

2.1. Inteligencia

En términos generales, la «Inteligencia» está «Concebida como un producto, esta tiene su base en la información (*conocimiento*), determinada como necesaria a través del planteamiento y dirección —presentes en todo el ciclo—, así como por los requerimientos formulados por los consumidores de Inteligencia que experimentan necesidades surgidas de acontecimientos súbitos o coyunturales.»⁵²

2.2. Sistemas de Inteligencia

Muchas de las necesidades humanas han requerido de sus propios sistemas de Inteligencia para la mejor satisfacción de tales necesidades; así, en la actualidad, es muy común constatar que existe Inteligencia económica, Inteligencia social, Inteligencia política, Inteligencia de Estado, etc.; no obstante, en general, todo sistema de Inteligencia está compuesto por un ciclo, «que comprende las fases de planeamiento y dirección; obtención y recolección; procesamiento, análisis y producción, así como distribución y difusión del conocimiento, que tiene como objetivo servir a los tomadores de las decisiones de índole económica, política, militar y social...»⁵³ No obstante, como mencioné arriba, el ámbito de esta investigación será la Inteligencia de Estado.

⁵² Pérez García, Juan Francisco, *Op. Cit.*, Pág 12-13.

⁵³ Pérez García, Juan Francisco, *Op. Cit.*, Pág. 45.

2.3. ContraInteligencia Cibernética

En un «Cuaderno de Lecturas» publicado por la Escuela de Inteligencia y Seguridad Nacional (ESISEN) de México, se hace la advertencia de que la mayoría de bibliografía disponible sobre temas de Inteligencia, está en inglés. Estas publicaciones se centran en las experiencias posteriores a la Segunda Guerra Mundial. En una de estas recopilaciones se afirma: «Es muy probable que este sea el primer cuaderno de lecturas que se genera en México sobre contraInteligencia, y probablemente en otros países de habla hispana.» Agrega el autor de la introducción: «Ello no es extraño, ya que la bibliografía disponible en español sobre Inteligencia es muy escasa, y la contraInteligencia, por su misma naturaleza, es un subtema de la actividad de la Inteligencia aún menos conocido.» Esta afirmación la refuerzan con la opinión de John Ehrman, uno de los autores incorporados en esa recopilación: «la contraInteligencia es un área de estudio relativamente ignorada por la comunidad de Inteligencia.»⁵⁴

Esta escasez principia por la misma Inteligencia, concebida como «una técnica para generar conocimientos y un conjunto de actividades». La consecuencia es que sea poco comprendida por quienes no tienen experiencia directa con las entidades estatales vinculadas con las distintas modalidades de seguridad. El grado de dificultad aumenta al abordar la ContraInteligencia.

Tanto la Inteligencia como la ContraInteligencia surgieron en el entorno de guerras entre ejércitos de diferentes países. Con el transcurso del tiempo, ambas

⁵⁴ En Introducción. «ContraInteligencia». Escuela de Inteligencia y Seguridad Nacional (ESISEN), Lecturas Básicas de Inteligencia, 2010, No. 4, pág. 13.

actividades se agenciaron de autonomía duradera, o sea, continuaron existiendo con independencia de que se dieran conflictos armados o no. En la actualidad, «incluye fundamentalmente la adopción de medidas defensivas por parte de un Estado contra distintos tipos de amenazas, que no son necesariamente ejércitos enemigos, sino otro tipo de adversarios.»⁵⁵

Son numerosos los hechos realizados por medios cibernéticos que han provocado confrontaciones entre Estados. Estos incidentes pudieron desembocar en situaciones de guerra cibernética. José María Molinos Mateos sostiene al respecto: «Actos de guerra cibernética podrían ser aquéllos que se producen cuando un ataque cibernético es realizado, apoyado o tolerado por un Estado; tiene motivación u objetivo político selectivo o explícito; se realiza de forma planificada; tiene una frecuencia y duración suficiente para asegurar el cumplimiento del objetivo perseguido, y sus daños directos o indirectos son graves.»⁵⁶

A partir de mediados de los años noventa del siglo pasado, se ha generalizado una nueva concepción de seguridad, de naturaleza multidimensional. Esta visión más amplia se propone superar las amenazas tradicionales y la defensa de carácter militar. Ha incorporado aspectos vinculados con la economía, la política, el terrorismo, el crimen organizado, las pandemias, el tráfico de drogas, las tecnologías, las migraciones, la estabilidad institucional, la cultura, el medio

⁵⁵ *Ibíd.*

⁵⁶ Molinos Mateos, José María. «ContraInteligencia cibernética». En: Fernando Velasco y Rubén Arcos (editores). «Cultura de Inteligencia: un elemento para la reflexión y la colaboración internacional.» Actas del Segundo Congreso de Inteligencia, Madrid, 22 – 24 de noviembre de 2010. Plaza y Valdés, 2012, pág. 82.

ambiente y el bienestar de los ciudadanos, así como otras de carácter «reputacional» que inciden en la imagen que un país proyecta en el exterior y que pueden tener graves repercusiones en los mercados financieros.

Las amenazas que acechan sobre el ciberespacio se originan en los Estados, los extremismos tanto ideológicos como políticos, el crimen organizado y la delincuencia individual. Estas contingencias tienen consecuencias significativas que afectan los derechos personales y las libertades individuales. En la actualidad, todas las actividades relacionadas entre individuos, grupos, gobiernos y entidades implican consecuencias, directas o indirectas, en el ámbito cibernético. Esto lo transforma en una senda forzosa para cualquier actividad de nuestros días y en recinto de atención constante de los servicios de Inteligencia y seguridad.

Para neutralizar los riesgos cibernéticos se requiere la aplicación de medidas encuadradas dentro de la Seguridad Cibernética. El citado autor Molinos Mateos formula la siguiente definición: «Seguridad cibernética técnica es el mecanismo destinado a prevenir un evento cibernético negativo o a limitar sus efectos. En un sentido político, seguridad cibernética sería la ausencia de amenazas cibernéticas que puedan poner en entredicho los valores centrales que una comunidad o una persona quiere preservar, y que entrañen un riesgo de empleo de fuerzas cibernéticas.»⁵⁷

La Inteligencia Cibernética es un resultado del procesamiento de información, ya sea real o latentemente hostil. Se realiza por medios cibernéticos, de igual manera que la actividad que la obtiene. La organización que tiene a su

⁵⁷ Ibídem, pág. 89.

cargo su desarrollo, se sustenta en lo esencial en la observación, intervención, análisis, manipulación y escucha de la World Wide Web o Internet.

La Inteligencia Cibernética, al igual que otro tipo de Inteligencia, está sujeta a limitaciones que perjudican, si bien de modo diferente, a la acción, al conocimiento, a la geografía, a la tecnología y a la confidencialidad. A todas estas hay que agregar las restricciones jurídicas procedentes de las tecnologías de la información y los elementos distintivos de la Seguridad Cibernética.

La mayoría de los elementos tecnológicos empleados en la Inteligencia Cibernética comprenden una tecnología refinada que no se encuentra al alcance de todas las instituciones y organizaciones. Si bien es cierto que la tecnología de punta se concentra en pocos países, no es exclusiva de ninguno, sino que radica en la Inteligencia humana, pero necesita de grandes esfuerzos de investigación y desarrollo (I+D) y de cooperación para concretarla.

La ContraInteligencia Cibernética consiste en el «mecanismo destinado a prevenir un evento cibernético negativo o a limitar sus efectos.» Al consistir en un conjunto de actividades dirigidas a establecer y neutralizar las amenazas de Inteligencia, «es una de las más importantes limitaciones con las que se encuentra la Inteligencia Cibernética para el logro de sus objetivos.»⁵⁸

Tanto la contraInteligencia como la seguridad cibernética comportan una organización que proteja sus activos cibernéticos de ataques que puedan representar una amenaza. Esto requiere la elaboración de doctrina,

⁵⁸ *Ibíd.*, pág. 89.

procedimientos, normas y medidas adecuadas para la protección que se pretende lograr.

2.4. Gestión del conocimiento y Servicios de Inteligencia

La información constituye un elemento primordial para el desarrollo. Con el transcurso del tiempo, la gestión de la información cada vez ocupa un espacio más amplio en la economía de los países a escala mundial. Bárbara Spiegelman, al plantear la necesidad inmediata de implantar modelos para la gestión de calidad en las instituciones de información, señala el vínculo estrecho existente entre gestión de la información, gestión del conocimiento y la calidad en el quehacer de una organización.

Al surgir la teoría de la organización, se incrementó la importancia de la información. Una organización es un sistema integrado por personas, recursos materiales e información, en la cual la última determina a los otros dos elementos. Por esta razón, las organizaciones son consideradas como sistemas de información. La gestión de información en las organizaciones ha sufrido una “revolución” debido al impacto de los cambios económicos, políticos, culturales, tecnológicos y otros. Es por eso que la base indispensable del nuevo modelo de gestión de información es la gestión del conocimiento.

Tal vez el “punto de inflexión” en los servicios de Inteligencia fue 2011. La carencia de Inteligencia o que no había una integración de los datos disponibles debido a una gestión defectuosa, fueron causas que no permitieron evitar los atentados del 11 de septiembre en Estados Unidos.

Se requieren soluciones para controlar las grandes cantidades de información que deben ser procesadas por los organismos de Inteligencia de un país y convertirlas en “conocimiento útil”. La gestión del conocimiento permite que la información sea recopilada y sistematizada.

Al respecto, Miguel Ángel Esteban Navarro y Diego Navarro Bonilla sostienen lo siguiente: «Si atendemos [...] el hecho de que la información obtenida por diversas fuentes es el elemento con el que se trabaja, descubrimos que estamos ante lo que se denomina en la actualidad un proceso de gestión del conocimiento. Sin embargo, la tradicional mutua ignorancia entre el cerrado y reservado mundo de los servicios de Inteligencia para la seguridad y la defensa, así como el abierto universo de la gestión de la información documental, dificulta la necesaria ósmosis de conocimientos y habilidades que enriquecería a ambas esferas. Su origen se encuentra, principalmente, en el diverso ámbito de aplicación de sus trabajos, los diferentes valores culturales que están detrás de los modos de adquisición, selección, tratamiento, difusión y uso de la información e incluso la procedencia y el estatus profesional de sus miembros.»⁵⁹

El uso de información por parte de los estados para la toma de decisiones sobre una base firme es una constante a través del tiempo. Por eso, la obtención y el análisis de información para su transformación en conocimiento aplicado que proteja contra amenazas internas o externas requiere de un repaso histórico para

⁵⁹ Navarro, Miguel Ángel Esteban, y Diego Navarro Bonilla. "Gestión del conocimiento y servicios de Inteligencia: la dimensión estratégica de la información." *El profesional de la información*, Vol. 12, No.4, 2003, págs. 269-281. Disponible en <<http://dialnet.unirioja.es/servlet/articulo?codigo=642870&orden=115896&info=link>>. Consultado el 20 de febrero de 2016.

comprender cómo funciona en la actualidad guatemalteca la gestión del conocimiento, como fundamento de la gestión de información.⁶⁰

3. Esbozo histórico de la Inteligencia en Guatemala

El origen de la Inteligencia de Estado en Guatemala, puede situarse a partir del régimen de Manuel Estrada Cabrera (1898-1920). Antes, en los regímenes de Justo Rufino Barrios, (1873-1885), Manuel Lisandro Barillas (1885-1892) y José María Reyna Barrios (1892-1898), se produjeron acciones de Inteligencia, pero se hicieron de manera asistemática; solo con Manuel Estrada Cabrera comenzaron a sistematizarse las acciones de Inteligencia.

3.1. El período liberal

El período de los liberales comienza, en Guatemala, con la llegada de la llamada «Revolución liberal» que abanderaron Miguel García Granados (1871-1873) y Justo Rufino Barrios (1873-1875). Durante el gobierno de García Granados comenzó a airearse la política guatemalteca al decretar la libertad de prensa, suprimirse las órdenes religiosas (en consecuencia los diezmos), y se expulsó a los jesuitas. No hubo, al principio, necesidad de organizar una Inteligencia de Estado ya que el gobierno se impuso por las armas; eso fue, al principio, un disuasivo contra sus adversarios y enemigos.

⁶⁰ Aja Quiroga, Lourdes. Gestión de información, gestión del conocimiento y gestión de la calidad en las organizaciones. ACIMED, Ciudad de La Habana, Vol. 10, No. 5, oct. 2002. Disponible en <http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352002000500004&lng=es&nrm=iso>. Consultado el 21 febrero 2016.

Justo Rufino Barrios esbozó una especie de Inteligencia elemental que estaba formada por quienes, con instrucciones de Barrios, lo informaban sobre los acontecimientos de interés en distintos puntos de la República. «... la red o grupo de informantes del gobierno de Justo Rufino Barrios no contó con ninguna experiencia previa en materia de Inteligencia, ni dispuso conceptualmente de una doctrina respecto del mismo, ni tampoco de un conocimiento de la función que debió cumplir dicha labor (Inteligencia) para servir a quienes condujeron el Poder del Estado (civiles y militares), y menos dispuso de una asesoría internacional en el tema, al menos es lo que se conoce hasta el presente. A diferencia de éste grupo de informantes, la estructura de los Jefes Políticos y Comandantes de Armas local (altos oficiales castrenses, ex miembros policíacos y algunos civiles) por haber formado parte de un Ejército forjado al calor de permanentes combates entre liberales y conservadores, debió disponer de un conocimiento teórico y empírico de lo que encierra una exploración de la posición enemiga.⁶¹ Igualmente, el desplazamiento de las unidades de combate o de la fuerza militar en su conjunto, para lo cual necesariamente tuvieron que recurrir a avanzadillas para asegurar los movimientos de su fuerza principal o del grueso de sus fuerzas.»⁶²

⁶¹ La exploración militar de una posición enemiga implica necesariamente una labor de Inteligencia. La búsqueda de información sobre la ubicación de su oponente armado en el teatro de operaciones, el número de sus integrantes, su volumen de fuego, la ubicación de sus postas y la hora en que realizan los relevos, entre otros datos. Información que es determinante para ejecutar el tipo de ataque armado que también estará en correspondencia con la ubicación y capacidad de respuesta que pueda tener el enemigo al que se desea atacar. (Pérez García, Juan Francisco, *Op. Cit.*, Pág. 180).

⁶² La avanzadilla es la efectuada por una pequeña unidad de combate que avanza al frente de la tropa y que tiene dentro de sus misiones garantizar que la fuerza principal o el grueso de sus fuerzas lleguen al destino previamente planificado. Pequeña unidad que debe disponer de información sobre los movimientos del oponente armado, de lo contrario, debe recopilarlos con núcleos poblacionales al momento de su desplazamiento. Interrelación que le permite a la

«... la red de informantes del gobierno de Justo Rufino Barrios puede anticiparse como el origen de los sistemas de Inteligencia del Estado guatemalteco»,⁶³ ya que basado en ellos pudo configurar un esquema de vigilancia que constituye una forma de Inteligencia primaria.

3.1.2. El gobierno de Manuel Estrada Cabrera

«Manuel Estrada Cabrera, enfrentado a un alto grado de inestabilidad económica y política, diseñó, sobre bases reales, una agenda de seguridad para hacer frente a las amenazas que se le presentaron en ambas estructuras o ámbitos.»⁶⁴

Durante este período gubernamental es reconocible un Ciclo de Inteligencia de cuatro fases:

1. Planificación y determinación de la acción de Inteligencia realizado por Manuel Estrada Cabrera.

2. Recopilación y obtención de la información que fue ejecutada por una red de espías que accionaron en todos los ámbitos de interés gubernamentales.

3. Sistematización, procesamiento y análisis para producir el conocimiento necesario para el gobernante que, se supone, estuvo a cargo de su hijo.

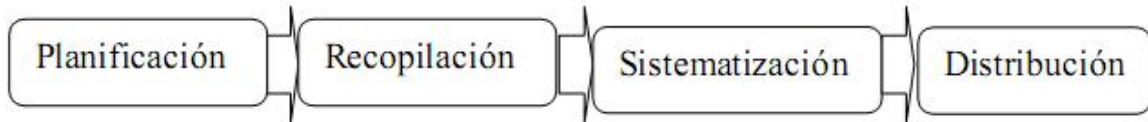
4. Distribución y difusión del conocimiento; «fue determinada por el Jefe del Ejecutivo, quien a su vez la diseminaba al jefe del aparato policíaco, al

avanzadilla identificar a las personas con las que se va construyendo una red de colaboradores que se transforma, con el paso del tiempo, en una red de información o de Inteligencia. Pero también la avanzadilla es la vigilancia que realizan dos o más efectivos guerrilleros a una distancia considerable del campamento, específicamente en la ruta que podría ser utilizada por una unidad castrense. (*Ídem*, Pág. 180).

⁶³ Pérez García, Juan Francisco, *Op. Cit.*, Pág. 213.

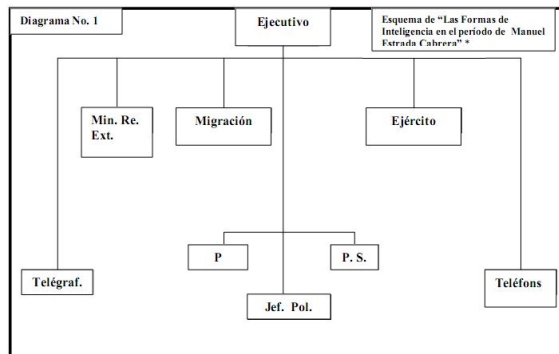
⁶⁴ *Ídem*, Pág. 43.

responsable del cuerpo de agentes secretos o policía política, así como a los responsables de los grupos de orejas y espías por departamento, con quienes mantuvo una comunicación directa.»⁶⁵



Ciclo de Inteligencia usado por Manuel Estrada Cabrera

«El tipo de Inteligencia que se desarrolló a lo largo del régimen de los veintidós años, dentro de las fronteras nacionales, fue la **Inteligencia Doméstica**,⁶⁶ como se le denomina actualmente; la cual tuvo como objetivo prevenir y enfrentar las amenazas de sus opositores, interesados en debilitar las capacidades del Estado guatemalteco para gobernar el país.»⁶⁷ El esquema de Inteligencia en el período de Manuel Estrada Cabrera se muestran en el siguiente gráfico, tomado del libro Juan Francisco Pérez:⁶⁸



⁶⁵ *Ídem*, Pág. 47

⁶⁶ El énfasis es mío.

⁶⁷ *Ídem*, Pág. 48

⁶⁸ Pérez García, Juan Francisco, *Op. Cit.*, Pág. 44

Ejecutivo; Migración; Ejército: Min. Re. Ext.: Ministerio de Relaciones Exteriores; P: Policía nacional; P. S.: Policía Secreta o Judicial; Jef. Pol.: Jefe Político local; Telégraf: Telégrafos; y Teléfons: Teléfonos.

3.1.3. Después de Estrada Cabrera

Los mandatarios que sucedieron a Estrada Cabrera siguieron, prácticamente, la misma tónica en materia de Inteligencia, con el agregado de que cada vez más se sintió la influencia norteamericana, que había comenzado a percibirse de manera evidente a partir del gobierno de Manuel Estrada Cabrera. A tal grado que, durante el gobierno de Jorge Ubico, que era simpatizante de los alemanes,⁶⁹ no pudo resistir la presión estadounidense que se dio, en el marco de la Segunda Guerra Mundial, y se vio obligado a expulsarlos de Guatemala. A partir de la extradición de los alemanes, los norteamericanos coparon casi todos los ámbitos productivos y económicos dejados por los europeos. Ocupados esos espacios, la intromisión norteamericana avanzó, incluso, hasta condicionar al gobierno a aceptar las políticas que ellos determinaran en la materia que fuere y, en consecuencia, a formar a los cuadros de Inteligencia que funcionaban en Guatemala; de paso, a infiltrarlos para poder maniobrar de mejor manera. No obstante, con la llegada de los gobiernos revolucionarios, la situación cambió por diez años. Al asumir el gobierno Juan José Arévalo (15 de marzo de 1945), el rumbo político varió al establecer las cuatro prioridades de su gobierno: «reforma agraria, protección del

⁶⁹ Schlesinger y Kinzer, en *Fruta Amarga* (Pág. 41), dicen que Ubico «había expresado simpatía por los nazis, hasta que fue reprendido en privado por los norteamericanos.»

trabajo, un sistema educativo mejor y consolidación de la democracia política.»⁷⁰

La Inteligencia de Estado en este período está poco documentada, en lo que respecta a Guatemala; no obstante, en el ámbito internacional sí puede verse un avance en cuanto a la sistematización y estudios sobre este aspecto, sobre todo a partir de la experiencia de la Segunda Guerra Mundial con el empleo, sobre todo, de los sistemas de Inteligencia utilizados por Alemania, Inglaterra, Francia, la URSS y Estados Unidos; esto, por supuesto, incidió posteriormente en Guatemala.

En Guatemala se realizó, en 2000, el Proyecto hacia una Política de Seguridad para la Democracia, que produjo el documento *Aportes para el estudio de la Inteligencia de Estado en Guatemala*; no obstante, no aborda el período de los dos gobiernos revolucionarios. Arranca, en el Capítulo II / Los antecedentes, diciendo solamente que «En el contexto de la guerra fría, los servicios nacionales de Inteligencia iniciaron un proceso de creciente profesionalización.»⁷¹

Durante el gobierno de Arévalo también se abrió un frente enemigo para la democracia guatemalteca: la United Fruit Company (UFCO) porque, «dueña de vastas tierras, el ferrocarril y el puerto, virtualmente exonerada de impuestos y libre de controles [en el gobierno de Arévalo], dejó de ser omnipotente en sus

⁷⁰ Schlesinger, Stephen y Kinzer, Stephen, *Fruta Amarga*, Siglo XXI Editores, cuarta edición en español, México, 1987, Pág. 50.

⁷¹ En este estudio participaron el Ministerio de la Defensa, el Ministerio de Gobernación, la Secretaría Administrativa y de Seguridad de la Presidencia, la Secretaría de la Paz, la Secretaría de Análisis Estratégico de la Presidencia, el Centro de Acción Legal para los Derechos Humanos, el Centro de Estudios de Guatemala, el Centro de Estudios Urbanos y Regionales de la Universidad de San Carlos de Guatemala, la Escuela de Ciencia Política de la Universidad de San Carlos de Guatemala, la Facultad Latinoamericana de Ciencias Sociales, la Facultad de Ciencias Políticas y Sociales de la Universidad Rafael Landívar, la Fundación Myrna Mack, el Instituto de Estudios Comparados en Ciencias Penales de Guatemala, el Instituto de Enseñanza para el Desarrollo Sostenible, el Instituto de Estudios Políticos, Económicos y Sociales, Seguridad en Democracia, Julio Balconi y Héctor Rosada.

propiedades. En 1951, en su discurso de despedida, Arévalo reveló que había debido sortear treinta y dos conspiraciones financiadas por la empresa.»⁷² En tal contexto, el Sistema de Inteligencia que sí funcionó fue el de Estados Unidos. Lo hizo, sobre todo, para cuidar los intereses de la UFCO; las acciones de Inteligencia se acentuaron contra Guatemala a partir de la presidencia de Jacobo Árbenz Guzmán. «Arbenz estaba decidido a transformar a Guatemala en un estado capitalista moderno», según las palabras de un historiador norteamericano, a “liberarla económicamente de la dependencia de los precios mundiales del café y arrancar el control de la economía de las corporaciones estadounidenses que lo retenían.»⁷³ Los de la UFCO se alarmaron y comenzaron a presionar con insistencia en todos los ámbitos del gobierno estadounidense para persuadir al gobierno guatemalteco de que estos cambios no debían darse, ya que afectarían sus intereses; en consecuencia, por ser la UFCO una empresa norteamericana, por extensión, estarían afectando los intereses de los norteamericanos. Fue una estrategia en la que insistió el embajador norteamericano Richard Patterson antes de abandonar Guatemala; lo hizo por medio de una carta que le envió a Sam Zemurray, quien era el representante de la UFCO en Guatemala y uno de sus grandes accionistas. «Patterson recomendaba que la United Fruit lanzara inmediatamente “fuego de artillería total sobre el Senado estadounidense acerca del mal trato que recibe el capital norteamericano en Guatemala. Esto quitará la

⁷² Eduardo Galeano, *Las venas abiertas de América*, Siglo XXI Editores, cuadragésimonovena edición, México, 1987, Pág. 181.

⁷³ Schlesinger, Stephen y Kinzer, Stephen, *Op. Cit.* Pág. 66.

responsabilidad a la UFCO y pondrá las bases para una demanda de nuestros senadores para que los intereses norteamericanos reciban un trato justo”.»⁷⁴

A la estrategia anterior se añadió, durante el gobierno de Árbenz, que este estaba «copado por comunistas». Para fortuna de la UFCO el presidente era Dwight Eisenhower, un declarado anticomunista, de quien estaban seguros no dudaría en aceptar una invasión a Guatemala para imponer los intereses de la UFCO. Eisenhower sabía mucho de Inteligencia Estratégica; fue quien dirigió el desembarco en Normandía que apresuró el final de la Segunda Guerra Mundial al conseguir el rendimiento de Alemania. La operación tuvo éxito, en buena medida, porque se hizo un gran trabajo de Inteligencia y ContraInteligencia; en consecuencia, se logró despistar al ejército alemán que no acertó a anticiparse a los movimientos norteamericanos.

Durante la presidencia de Truman, la UFCO había conseguido montar una operación para invadir Guatemala pero, cuando iba a concretarse, el presidente la abortó. Con Eisenhower estaban seguros de que esto no sucedería. La estrategia era atacar un punto muy sensible en la política norteamericana de entonces: el comunismo. Después de la presión que se había ejercido contra Arévalo, se montó un enorme aparato propagandístico para convencer a los norteamericanos de que el gobierno de Árbenz era «comunista». Los gobiernos de Arévalo y el de Árbenz no tuvieron la capacidad para contrarrestar la propaganda y la embestida estadounidense contra los gobiernos revolucionarios, que se arreció con Árbenz.

⁷⁴ Schlesinger, Stephen y Kinzer, Stephen, *Op. Cit.* Pág. 97.

Durante el primer gobierno revolucionario, el embajador estadounidense Richard Patterson, «que no hablaba español y era proclive a describir vívidamente la amenaza del comunismo soviético en Guatemala, había chocado repetidamente con el gobierno de Arévalo. Insistía una y otra vez en que Arévalo destituyera a varios ministros de su gabinete por ser “comunistas” e, incluso comenzó a reunirse con conspiradores que intentaban derrocar al presidente. Finalmente el gobierno [guatemalteco] lo declaró *persona non grata* y fue depuesto en abril de 1950.»⁷⁵

Durante el segundo gobierno revolucionario la presión norteamericana se hizo más fuerte; sobre todo por la puesta en marcha del *Decreto 900, Ley de Reforma Agraria* que afectó de manera directa los intereses de la UFCO, al serle expropiadas grandes extensiones que esta empresa mantenía ociosas. El embajador guatemalteco en Washington, Guillermo Toriello, defendió por todos los medios a su alcance la posición soberana de Guatemala al emitir tal ley. «Desmentía que fuera discriminatoria contra la United Fruit, según acusaba ésta, y afirmaba que la compensación ofrecida era justa puesto que se basaba en las propias tasaciones de la empresa sobre el valor de la tierra en sus declaraciones de impuestos. Señalaba que las expropiaciones beneficiaban a un gran número de campesinos sin tierras que vivían en una miseria extrema, y que además ponía fin a las injustas concesiones otorgadas a la compañía por Estrada Cabrera y Ubico.»⁷⁶

⁷⁵ Schlesinger, Stephen y Kinzer, Stephen, *Op. Cit.* Pág. 97.

⁷⁶ Schlesinger, Stephen y Kinzer, Stephen, *Op. Cit.* Pág. 117.

En esa pugna y convencido por el Secretario de Estado John Foster Dulles, el presidente Eisenhower le dio un giro a la Agencia Central de Inteligencia (CIA), de la cual era director Allen W. Dulles, hermano de John Foster Dulles, ya que utilizar a tal Agencia «como instrumento de la intervención política constituyó una ruptura con las prácticas del presidente Truman que se había servido de la CIA sobre todo para recabar información.»⁷⁷ El presidente Árbenz renunció, por medio de la radio nacional TGW; en su alocución se preguntó y al mismo tiempo respondió: «¿En nombre de qué hacen estas barbaridades? ¿Cuál es su bandera? Todos la conocemos también. Han tomado de pretexto al comunismo. La verdad es muy otra. La verdad hay que buscarla en los intereses financieros de la compañía frutera y en los de los otros monopolios norteamericanos que han invertido grandes capitales en América Latina, temiendo que el ejemplo de Guatemala se propague a los hermanos países latinoamericanos.» Justificó su renuncia de la manera siguiente: «Como mi gobierno ha sido acusado de ser de naturaleza comunista, sin que hayamos podido desvanecer que no lo es, aún cuando hemos empleado todos los medios para convencer a los elementos reaccionarios del mundo de que lo sostenido por los círculos gobernantes norteamericanos es una patraña, y como esos círculos harán más despiadada la agresión contra Guatemala, he tomado una dolorosa y cruel determinación: Después de meditarlo con una clara conciencia revolucionaria, he tomado una decisión de enorme trascendencia para nuestra patria, en la esperanza de detener la agresión y devolverle la paz a Guatemala. He determinado abandonar el poder

⁷⁷ Schlesinger, Stephen y Kinzer, Stephen, *Op. Cit.* Pág. 111.

y poner el mando del ejecutivo de la nación en manos de mi amigo el coronel Carlos Enrique Díaz, jefe de las Fuerzas Armadas de la República.»

El designado por Jacobo Árbenz para sustituirlo, Carlos Enrique Díaz de León, solo ejerció el cargo durante un día. Después se constituyeron dos Juntas de Gobierno y el 8 de julio de 1954, los norteamericanos designaron a Carlos Castillo Armas para estar al frente del Gobierno, siempre que no se saliera del rumbo que se le había asignado ya que ellos “lo habían reclutado, adiestrado y pagado a sus hombres”...»⁷⁸ En su momento, los norteamericanos esgrimieron el argumento de que eran ajenos a la invasión. El mismo embajador John E. Peurifoy lo negaba, siendo él mismo uno de las principales personas que alentó el golpe contra la soberanía del Estado de Guatemala. Por eso, Guillermo Toriello lo llamó «truhán».⁷⁹ No obstante, la historia se encargó de aclarar dicha intromisión. Entre los muchos documentos y testimonios respecto a la participación del gobierno estadounidense, está el siguiente: «Se hizo contacto con los principales elementos de la oposición guatemalteca y, finalmente, se escogió como el mejor instrumento del plan UFCO-Departamento de Estado-CIA a Carlos Castillo Armas, exmilitar que se había rebelado contra el gobierno de Guatemala (octubre, 1950) Y se hallaba en Honduras. Un abogado en New Orleans era el agente de enlace, pagaba las planillas mensuales de la conspiración y las compras de material bélico. Castillo Armas, a su vez, mantenía un agente confidencial ante el Departamento de Estado (pagado por él con los mismos fondos que recibía de la

⁷⁸ Schlesinger, Stephen y Kinzer, Stephen, *Op. Cit.* Pág. 38.

⁷⁹ Toriello, Guillermo, *La Batalla de Guatemala*, Editorial Universitaria, Universidad de San Carlos de Guatemala, Guatemala, 1997, Pág. 73.

UFCO).»⁸⁰ Luego, para reafirmar su aserto, dice: «Armas, municiones, aviones del Gobierno de Estados Unidos, material bélico de toda clase, abastecimiento e impedimenta, pilotos y mecánicos de aviación estadounidenses, mercenarios, Castillo Armas, millones de dólares en juego, inaudita tolerancia de Honduras y Nicaragua, barcos equipados para operaciones comando, etc. ¿A quién se le podría hacer creer que todo esto sucedía sin la complicidad del Gobierno de Estados Unidos?»⁸¹

Luego de esta larga relación de los hechos, pero necesaria para entender el contexto en el cual se dio lo que trataré en un apartado posterior, entre muchas más, quedan las siguientes dos preguntas por contestar:

- ¿Por qué Guatemala no utilizó e hizo eficiente un Sistema de Inteligencia en el período revolucionario?
- ¿Por qué si las tropas con las cuales ingresó el «ejército» de Castillo Armas era muy inferior al Ejército de Guatemala y, además, había sido derrotado en sus dos terceras partes, pudo triunfar y hacerse con el poder?

A la primera pregunta, a la luz de la historia, podemos inferir que, en el período del presidente Arévalo, privó en los primeros dos años de su gobierno una confianza absoluta e ingenua de que, dada la abrumadora cantidad de votos con los que ganó las elecciones (85%), el pueblo respaldaría su gobierno ante cualquier amenaza. En tal sentido, un Sistema de Inteligencia se hacía innecesario, sobre todo por el espíritu democrático que animaba a Arévalo y por

⁸⁰ Toriello, Guillermo, *Op. Cit.*, Págs. 73-74.

⁸¹ Toriello, Guillermo, *Op. Cit.*, Pág. 75.

su idealista confianza en el ser humano y en que se respetaría el voto que se le concedió. «La imponente presencia de Arévalo como símbolo de la revolución de Octubre bastó para mantener un grado de estabilidad en los primeros años. Pero a la mitad de su período, en 1948, empezó a crecer la inquietud. A pesar de sus buenas intenciones, Arévalo no tenía un programa coherente para después de su primer asalto de reformas y su base política de discusiones se estaba erosionando.»⁸² Arévalo fue consciente de esa situación a la que contribuyeron, incluso, personas de su confianza en las altas esferas de su gobierno. «La despedida de Juan José Arévalo el 15 de marzo de 1951, en la toma de poder de Arbenz, sin embargo, fue un tenebroso avalúo del estado político del país. [...] El desilusionado Arévalo reconoció que su sucesor, o bien tendría que abandonar los ideales de la revolución de Octubre totalmente, o bien presionar para consolidarlos. [...] Pero al defender los ideales revolucionarios, Arbenz parecía destinado, según temía Arévalo, a incitar lo que él había llamado “esa fuerza anónima” contra él y contra la revolución que había ayudado a iniciar con tan altos ideales.»⁸³ Sin embargo, al asumir Arbenz el gobierno, tampoco implementó un Sistema de Inteligencia que fuera capaz de advertir y prevenir las amenazas contra su gobierno. Esto que le sucedió a los dos gobiernos revolucionarios tiene también otra explicación: la Inteligencia de Estado, en sentido estricto, no se había practicado a cabalidad en los gobiernos anteriores; y, menos, sistematizado de manera adecuada. En ese sentido, la ventaja estadounidense era que ellos sí la

⁸² Schlesinger, Stephen y Kinzer, Stephen, *Op. Cit.* Pág. 53.

⁸³ Schlesinger, Stephen y Kinzer, Stephen, *Op. Cit.* Pág. 61.

habían practicado, sobre todo con especial empuje y tecnología innovadora a partir de la Segunda Guerra Mundial; además, poseían una agencia especial encargada, no solo de practicar la Inteligencia sino de sistematizarla e implementarla con la rapidez de los avances tecnológicos que en ese ámbito se habían generado.

La respuesta a la segunda pregunta planteada tiene mucho qué ver con la respuesta a la primera. Podemos inferir que Árbenz, a pesar de poseer una fuerza militar superior para enfrentar a las tropas mercenarias⁸⁴ con «6 000 hombres y su fuerza policíaca de 3 000 en estado de alerta, pero decidió conservar la fuerza del ejército en reserva, acuartelando a la mayoría de las tropas hasta nueva orden.»⁸⁵ Perdió por muchas más causas de las que enumero pero, en primer lugar, por no poseer un Sistema de Inteligencia que fuese capaz de proveer información, veraz, exacta y adecuada sobre unas tropas que, en otras circunstancias, habrían sido fácilmente derrotadas; en segundo, por las traiciones que se dieron dentro del propio ejército y dentro de sus funcionarios;⁸⁶ en tercero porque los norteamericanos no escatimaron recursos para financiar a las tropas mercenarias

⁸⁴ «Desde el 17 de junio en la noche un puñado de mercenarios, entre 256 y 300 hombres a lo sumo (Hurtado Aguilar, 1956 p. 181; Del Valle Matheu, 1956, p. 138; Gleijeses, 1991, p. 320) pagados por la CIA y encabezados por el coronel Carlos Castillo Armas, penetró en el territorio guatemalteco por el departamento de Chiquimula.» Citado en: Figueroa Ibarra, Carlos, *Paz Tejada / militar y revolucionario*, Editorial Universitaria, Universidad de San Carlos de Guatemala, Guatemala, 2001, Pág. 263.

⁸⁵ Schlesinger, Stephen y Kinzer, Stephen, *Op. Cit.* Pág. 24.

⁸⁶ El desmoronamiento de la lealtad del Alto Mando del Ejército para con Árbenz, era advertible desde el 8 de junio cuando la oficialidad le entregó un cuestionario al presidente: de las 20 preguntas que muestra un artículo periodístico transcrito en una fuente anticomunista, *El Libro Negro del Comunismo en Guatemala*, casi la mitad tenían que ver directamente con el comunismo y el resto lo hacía de manera indirecta (CPPCISAL, s/f, pp. 173-180).» Citado en: Figueroa Ibarra, Carlos, *Paz Tejada / militar y revolucionario*, Editorial Universitaria, Universidad de San Carlos de Guatemala, Guatemala, 2001, Pág. 264.

y, en cuarto, porque el presidente Árbenz se dio cuenta «gradualmente de que Estados Unidos apoyaba a los rebeldes y de que una respuesta militar temeraria podría ser suicida.»⁸⁷ La guerra de Vietnam aun no sucedía; de lo contrario, Árbenz hubiese tenido más elementos de juicio para ejercer la defensa ante la invasión mercenaria ya que el ejército vietnamita era considerablemente menor que el norteamericano; las armas y la tecnología de guerra vietnamita también eran muy inferiores; no obstante, según las enseñanzas de Sun Tzu, en *El arte de la guerra* (Pág. 27), entendió que «de gran importancia en la guerra es combatir la estrategia del enemigo.» Por eso, la Guerra de Vietnam fue uno de los grandes fracasos estratégicos de Estados Unidos porque Vietnam supo sacar la guerra de su territorio y llevarla al estadounidense. No con armas convencionales de la guerra sino por los medios de comunicación y con el conocimiento e información que tenía de su enemigo. Fue capaz de hacerle entender a la opinión pública y a los norteamericanos de que la guerra que su ejército estaba librando era inútil, costosa económicamente y, sobre todo, muy costosa en vidas humanas de miles de norteamericanos. Ante esa estrategia, que supuso el uso de un afinado aparato de Inteligencia Estratégica, los vietnamitas no solo sacaron la guerra de su territorio sino que además de llevarla a suelo norteamericano, lograron que Estados Unidos se retirara de ese país asiático.

⁸⁷ Schlesinger, Stephen y Kinzer, Stephen, *Op. Cit.* Pág. 38.

3.2. Después de 1954

El 13 de noviembre de 1960 se dio el levantamiento armado de miembros del Ejército. El alzamiento se desarrolló en el marco de la Guerra Fría, «y que no es más que la confrontación militar, económica, política, diplomática y psicológica, planetaria entre los Estados Unidos y la Unión Soviética, dos modelos económicos y políticos antagónicos —capitalismo y socialismo— en escenarios externos a ambas potencias.»⁸⁸

Al concluir la Segunda Guerra Mundial, los Países Aliados,⁸⁹ que vencieron a los países agrupados como las Potencias del Eje,⁹⁰ decidieron ejercer su liderazgo de vencedores sobre los territorios de los vencidos y en las regiones que estos habían invadido o sometido. No obstante, las fuerzas principales que disputaron el control de estos territorios y deseaban que sus sistemas económicos, políticos y sociales, tuviesen primacía fueron la Unión Soviética y Estados Unidos. Luego que fueron aliados en la guerra declarada, se hicieron antagónicos en una guerra no declarada y que se libró casi de manera sorda y secreta, por lo cual dio en llamarse Guerra Fría.

A partir de 1954, las directrices en nuestro país se enmarcaron dentro de la denominada «Doctrina de Seguridad Nacional». Así lo reconoció Alejandro Gramajo (1989), quien entonces era Ministro de la Defensa: «La Doctrina de Seguridad Nacional, fue prácticamente un “injerto” de realidades de países

⁸⁸ Pérez García, Juan Francisco, *Op. Cit.*, Pág. 9

⁸⁹ Esta coalición estuvo integrada, fundamentalmente, por la Unión Soviética, Estados Unidos, el Reino Unido y Francia.

⁹⁰ Este grupo lo integraron Alemania, Italia y Japón.

desarrollados a países en desarrollo como Guatemala; los cuales adoptándola la aplicaron cada uno a su modo.»⁹¹ Dentro de este ámbito que configuró el primer Sistema de Inteligencia que funcionó a cabalidad en Guatemala. Todo lo anterior que se practicó en Inteligencia de Estado fueron atisbos, aproximaciones. Se configuró un Sistema de Inteligencia de una guerra irregular, tal como conceptualizaron los ideólogos franceses David Galula y Roger Trinquier. La finalidad de este Sistema de Inteligencia era la defensa del Estado.

Antes de finalizar su gobierno, Enrique Peralta Azurdia creó la Agencia Presidencial de Inteligencia, la cual quedó bajo el control de *La regional*. Denominación que cambió, luego de asumir la administración de gobierno, el civil César Méndez Montenegro (1966-1970), por el de Servicio de Seguridad Nacional de Guatemala (SSNG).»⁹²

La preponderancia del Ejército duró, en la práctica, hasta que el Estado guatemalteco se reacomodó, después de haberse firmado, el 29 de diciembre de 1996, el último de los *Acuerdos de Paz*: el *Acuerdo de Paz Firme y Duradera*.

Regresando históricamente, cuando Castillo Armas estuvo al frente del gobierno todavía se tenía el concepto de que la guerra era la confrontación de un ejército regular contra otro regular y se libraba en el campo de batalla; todavía se conservaba el modelo utilizado en la Primera y Segunda Guerras Mundiales. La estrategia estaba en función de esa conformación de la guerra; la Inteligencia de Estado, en buena medida, seguía el patrón que se había afianzado en la Segunda

⁹¹ Gramajo Morales, Héctor Alejandro, *Tesis de la Estabilidad Nacional*, Editorial del Ejército, Guatemala, 1989, Pág. 38.

⁹² Pérez García, Juan Francisco, *Op. Cit.*, Pág. 94.

Guerra Mundial. Así se enseñaba desde la Escuela Politécnica. No obstante, sucesos como la Guerra en la entonces llamada Indochina (Camboya, Laos, Vietnam del Norte y Vietnam del Sur) que se libró entre 1945 y 1954, y la Guerra de Independencia en Argelia (1954-1962), ambas contra el colonialismo francés, supusieron un cambio radical en la guerra y su estrategia; ya no se planteó en términos de guerra regular sino como guerras de guerrillas que, en la actualidad, también se le incluye dentro de las formas de guerra que técnicamente se denomina como Guerras de Cuarta Generación o Guerras Asimétricas.⁹³ El escenario no suponía ni campos de batalla, ni grandes frentes de guerra. El enemigo a derrotar no era fácilmente localizable, se desplazaba con suma facilidad, estaba muy organizado y actuaba donde menos se esperaba. Lo paradójico era que ese enemigo irregular, no contaba con armas adecuadas, era numéricamente inferior y la tecnología de guerra con la que contaba era desproporcionadamente inferior; sin embargo, las estrategias para vencerlo resultaban ineficaces. En consecuencia, el Ejército debía mantenerse en permanente estado de alerta. Esa nueva forma de hacer la guerra a las fuerzas no convencionales, en buena medida, fue pensada por los franceses, que la idearon

⁹³ «El concepto de Guerra de Cuarta Generación es tan solo el paso preliminar para construir el concepto de Guerra Asimétrica. En ese sentido, las discusiones de Cuarta Generación están limitadas solo al planteamiento amenazante de actores irregulares y terroristas a estados, así como a la respuesta extra territorial que un Estado hace a amenazas privadas, organizaciones terroristas o movimientos irregulares.

»El concepto de Guerra Asimétrica es un poco más elaborado, ya que incluye dimensiones no militares en las respuestas de Estados, relegando el esfuerzo militar a un segundo plano. No obstante, especifica que la respuesta desde el Estado debe ser total, o sea incluir todos los medios de poderío estatal (incluso ilegales), mientras que la acción del bando débil es siempre prolongada, irregular y más política y mediática.» (Universidad Militar Nueva Granada, Instituto de Estudios Geoestratégicos y Asuntos Políticos, *Serie Informativo: Frente Externo*, No. 108, Pág. 4, consultado el 2-7-2014, a las 16:00 en: <http://www.iegap-unimilitar.edu.co/dmdocuments/info108cuartag.pdf>).

para sus guerras coloniales. En ese contexto hubo dos teóricos que repararon en esa nueva forma de guerra y observaron con detenimiento su proceso: Roger Trinquier y David Galula. Sus ideas fundamentales las expusieron en dos libros que, después, sirvieron para formar a los oficiales y soldados que enfrentarían las guerras irregulares que se dieron, sobre todo, en América Latina; por supuesto, en Guatemala. Roger Trinquier escribió *La guerra moderna* y David Galula *La lucha contra la insurrección. Teoría y práctica*. Luego, a pesar del fracaso de los franceses tanto en Indochina como en Argelia, fueron ellos quienes instruyeron a los norteamericanos en este tipo de guerra «antisubversiva», a quienes tampoco les funcionó en la guerra de Vietnam (1959-1975), en donde fracasaron y a un costo enorme, tanto material como en vidas humanas. Este nuevo concepto y estrategias de la guerra contrasubversiva llegaron a América a través, sobre todo, de la capacitación que los franceses dieron a los ejércitos de América, incluyendo a militares norteamericanos, sobre la forma de vencer a los enemigos que planteaban una guerra irregular, como la guerra de guerrillas. «... La Escuela de Guerra de París es su principal difusora. Los primeros interesados son argentinos. Entre ellos, el general López Aufranc, que participará en el golpe de 1976.»⁹⁴

Lo novedoso de la escuela francesa fue plantear que el enfrentamiento entre las fuerzas opositoras ya no era el campo de batalla. Ahora la lucha se daba en la población. Roger Trinquier lo explica así: «Las escuelas militares encargadas de enseñar la clásica doctrina de la guerra descansan en una serie de factores interesantes: la misión, el enemigo, el terreno y los recursos. Pero, por lo general,

⁹⁴ Marie Monique Robin, *Escuadrones de la muerte, la escuela francesa*.

omiten un factor que nosotros consideramos esencial en la guerra moderna: el habitante.»⁹⁵ La influencia de la escuela francesa llegó, sobre todo, del asesoramiento argentino al ejército de Guatemala. Debemos recordar que: «Los argentinos introdujeron el rastreo computarizado de llamadas telefónicas y revisión de facturas de luz y otras cuentas de servicios. Esta técnica ayudó a identificar casas de seguridad de la guerrilla basada, por ejemplo, en un alto grado de consumo de energía eléctrica.»⁹⁶

Debe recordarse que «fue a partir del Gobierno de Romeo Lucas García (de julio de 1978 a marzo de 1982) que muchas de ellas [características de la Inteligencia] empezaron a definirse de manera más clara y se consolidaron como particularidades propias de este sistema. Esto ocurrió así, ya que a partir de 1979 se inició una mayor profesionalización de la Inteligencia y se la fortaleció para utilizarla con sentido estratégico. [...] fue durante este Gobierno que la Inteligencia alcanzó un profundo conocimiento de las organizaciones guerrilleras; una mejor dotación de recursos de todo tipo; amplió su red de informantes; utilizó a la Policía para sus propios objetivos, y comenzó a ejercer un control más efectivo en las esferas militares, estatales y sociales.»⁹⁷ En general, el instrumento orientador del Ejército fue el *Manual de guerra contrasubversiva* que, a través del Centro de Estudios Militares, elaboró el propio Ejército de Guatemala con inspiración total en la experiencia francesa. Por parte de la guerrilla revolucionaria, cuando esta se

⁹⁵ Trinquier, Roger, *La guerra moderna*, Ediciones Cuatro Espadas, Argentina, 1981, Pág. 44.

⁹⁶ Comisión para el Esclarecimiento Histórico, *Guatemala, memoria del silencio*, Tomo II, Guatemala, 1999, Pág. 100.

⁹⁷ Comisión para el Esclarecimiento Histórico, *Op. Cit.*, Tomo II, Pág. 76

consolidó, se inspiró, sobre todo, en la experiencia guerrillera cubana; en consecuencia, una de las guías teóricas para su desempeño fue *La guerra de Guerrillas*, que Ernesto “Che” Guevara preparó en 1960. Enumeraré las características más destacadas, teniendo en cuenta que cada guerra de esta naturaleza, *per se*, tiene las propias.

1. En primer lugar, era una guerra irregular.

2. El enemigo no era un ejército convencional, fácilmente identificable y localizable. Ya lo decía el coronel Charles Lacheroy: «No se hace una guerra revolucionaria con un ejército organizado en divisiones, no se hace una guerra revolucionaria con una administración de tiempos de paz, no se hace la guerra revolucionaria con el código napoleónico.»⁹⁸

3. El campo de guerra de este nuevo tipo de guerra también era la población. Si bien los servicios de Inteligencia siempre fueron importantes en el ámbito de la guerra, ahora, de manera especial, eran indispensables porque se trataba de enfrentar a un enemigo del cual se desconocían muchos aspectos; entre otros, número de militantes, localización, trayecto de su movilidad, armamento, estrategias, etc.

4. La Inteligencia de Estado fue el elemento fundamental para la guerra contrasubversiva. La obtención de información constituyó una de las piezas vertebrales para las instituciones de seguridad.

⁹⁸ Robin, Maier-Monique, *Los escuadrones de la muerte. La escuela francesa*, Editorial Sudamericana, Argentina, 2005, Pág. 72.

5. Control social. En 1981 se crearon las Patrullas de Autodefensa Civil. Trinquier lo especifica muy claramente: «la meta final de la guerra moderna es el control de la población.»⁹⁹

6. A partir del control social y del conocimiento de las características del enemigo, demarcar las zonas enemigas y las amigas por color: la zona roja si los guerrilleros controlaban a la población. Las zonas rosada estaba constituida por aquellas poblaciones que, sin estar controladas por la guerrilla, sí le proporcionaban algún apoyo. Las zonas blancas, aquellas que eran afines al gobierno y al Ejército.

7. El conocimiento del contexto cultural y religioso. Uno de los elementos de Inteligencia Estratégica fue conocer el contexto cultural y religioso en el cual se desarrollaba el pueblo de Guatemala. Desde 1945, la Iglesia Católica se había manifestado anticomunista. En una Carta Pastoral Colectiva del Episcopado de la Provincia Eclesiástica de Guatemala (1 de octubre de 1945), los obispos se manifestaron así: «A los confiados e imprudentes que con todo y decirse católicos y perteneciendo tal vez a piadosas Asociaciones creen todavía en la inocencia de las doctrinas comunistas, amonestamos con la autorizada voz de Pío XI: “El Comunismo enseña y pretende, no oculta y disimuladamente, sino clara, abiertamente y por todos los medios, aún los más violentos, dos cosas: la lucha de clases encarnizada, y la desaparición completa de la propiedad privada. Para conseguirlo, nada hay a lo que no se atreva, ni nada que respete y, una vez conseguido su intento, tan atroz e inhumano se manifiesta, que parece cosa

⁹⁹ Trinquier, Roger, *Op. Cit.*, Página 111.

increíble y monstruosa.» Años después, «En 1953, Rossell envió la venerada imagen del Cristo Negro de Esquipulas, el lugar de peregrinaje más visitado de Guatemala, en una excursión antiarbenquista por todo el país y en abril de 1954, publicó una carta pastoral llamando explícitamente a “una cruzada sincera contra el comunismo”. Después del golpe, estas actividades le permitieron a la Iglesia afirmar que ella había desempeñado un importante papel en el derrocamiento de Arbenz, mostrándole a Rossell que la mejor manera de servir a Dios y a sí mismo era utilizar las técnicas pastorales de la iglesia para promover en Guatemala los planes de la guerra fría.»¹⁰⁰ Instruido sobre lo anterior, desde que Castillo Armas ingresó, proveniente de Honduras, a Guatemala, una de las primeras acciones que ejecutó fue permanecer en Chiquimula; específicamente en Esquipulas. Allí, en el curso de una misa que se celebró en el templo de Esquipulas, Castillo Armas declaró al «Señor de Esquipulas» como «Capitán General del Ejército de Liberación». Y con Castillo Armas en el gobierno, el arzobispo Rossell fue condecorado.

8. Evitar la conjunción del enemigo interno con el externo. Este era uno de los asuntos más importantes; en otras palabras, se debía evitar a toda costa que el llamado enemigo interno tuviera relación o lazos de unión con el enemigo externo, grupo dentro del cual estaban involucrados, por ejemplo, Cuba y la Unión Soviética.

¹⁰⁰ Carlota McAllister en: Spencer, Daniela (compiladora), *Espejos de la guerra fría: México, América Central y el Caribe*, Centro de Investigaciones y Estudios Superiores en Antropología Social, México, 2004, Pág. 258.

9. Introducir el concepto de guerra psicológica para ganar adeptos. «La manipulación de la información fue otro de los procedimientos y de las finalidades utilizadas por la Inteligencia. Esta podía tener múltiples objetivos, desde emplearse como una técnica contra el enemigo hasta usarse para controlar a los medios de comunicación.»¹⁰¹

Hay muchos aspectos más pero, para el objetivo de esta investigación, considero suficientes las enumeradas en este apartado.

Durante el gobierno de Marco Vinicio Cerezo Arévalo (1986-1991) se iniciaron las conversaciones de paz, entre el Gobierno de Guatemala y la Unidad Revolucionaria Nacional Guatemalteca (URNG), que concluyeron en un proceso de negociación que llevó a la firma de los *Acuerdos de Paz* (29-12-1996). Eso obligó al Estado de Guatemala a recomponer su Sistema de Inteligencia. Eso derivó en buena medida de los numerales 47 al 52 del *Acuerdo sobre el Fortalecimiento del Poder Civil y Función del Ejército en una Sociedad Democrática*, firmado en México, el 19 de septiembre de 1996.

3.3. La llegada de la Informática

«Las primeras plataformas informáticas que se instalaron en el país fueron para la Inteligencia militar, que contó con modernos equipos de transmisión, equipos de escucha tanto fijo como móvil, incluso inalámbrico. En 1979, técnicos de una empresa israelita instalaron un centro de informática usado por la Regional. Dos

¹⁰¹ CEH, *Op. Cit.* Tomo II, pág.82.

años más tarde quedó concluida la Escuela de Transmisiones y Electrónica del Ejército, que fue equipada con el apoyo de Israel en 1981.»¹⁰²

El proceso manual que hasta la tercera parte del siglo XX fue común no solo en la recolección de la información sino en el análisis y distribución, cambió de manera radical cuando el siglo XXI se avecinaba; no obstante, ese cambio sustancial no tardó mucho en consolidarse en el área de Inteligencia del Estado pero se concentró, primero, en el Ejército; en las demás instituciones vinculadas con la seguridad, tardó un poco en consolidarse; el problema fue que cada institución, sobre todo a partir de la suscripción de los *Acuerdos de Paz*, ha manejado la información de manera separada y desconectada de un Sistema Nacional de Seguridad, en la cual toda la información pueda ser compartida y, de esa manera, ser institucionalmente más eficaces.

Aún en la época actual en muchas dependencias gubernamentales, a pesar del enorme avance tecnológico, los datos e información se recolectan de manera mecánica y, hasta manual. Eso dificulta su utilización y, en consecuencia, retarda los procesos. Aun en las instituciones gubernamentales en donde los procesos de recolección, análisis y distribución de la información se han automatizado, su uso se restringe solo a la institución que la recolecta. No se comparte con otras instituciones; o si se hace, implica mucha burocracia y, en consecuencia, tardanza. Es como si fueran feudos dentro de un Estado. En tal sentido, aunque cada institución cuente con la más sofisticada tecnología para el recaudo de la información, si esta no fluye de la manera más adecuada, implica subutilización de

¹⁰² Pérez García, Juan Francisco, *Op. Cit.* Págs. 113-114.

recursos técnicos y humanos; en consecuencia, poca eficacia para cumplir con las razones teleológicas de la Inteligencia de Estado.

La llegada de la informática al país, y posteriormente la aparición de las computadoras personales supuso un enorme avance; «lo importante [en el ámbito institucional] es seleccionar la que posibilite la compatibilidad de los sistemas que en la actualidad manejan las instituciones de seguridad y justicia...»¹⁰³ para eso deberán considerarse «como criterios principales la integridad de la información proveniente de las diferentes instituciones fuente; la visualización y el análisis de forma sencilla para los usuarios finales y la ubicación espacial de los eventos delictivos»¹⁰⁴ que repercuten en el Estado de Guatemala. En resumen, la llegada de la informática supuso un salto enorme y una herramienta valiosa para el proceso de recolección, análisis y difusión de la información; si no se hubiese contado con ese elemento, el rumbo de la guerra que sufrimos en el siglo pasado quizá habría tenido otro desenlace; no obstante, el asunto es que ese gran avance tecnológico aun es sub utilizado. Eso constituye, en muchos aspectos, un lastre para el efectivo desempeño de la Inteligencia de Estado.

3.4. En la actualidad

Al firmarse la paz en Guatemala, el cambio fundamental fue la variación de la razón teleológica de la Inteligencia de Estado. En ese sentido, el Estado se

¹⁰³ Bosos Monroy, Mario Alfredo y Cabrera Leonardo, César Augusto, *Principios de Unificación de los Servicios de Información de la PNC, para la creación de una Red de Seguridad Preventiva*, Universidad Galileo, Guatemala, 2010, Pág. 5.

¹⁰⁴ Bosos Monroy, Mario Alfredo y Cabrera Leonardo, César Augusto, *Op. Cit.* Pág. 5.

reconstituyó no para defenderse exclusivamente sino, de manera fundamental, para cumplir con su fin supremo: «la realización del bien común.»¹⁰⁵ También, para «garantizarle a los habitantes de la República la vida, la libertad, la justicia, la seguridad, la paz y el desarrollo de la persona.»¹⁰⁶

El cambio fundamental del Estado que se dio a partir del cese de la guerra fue concentrar su atención en los habitantes guatemaltecos, lo cual implicó modificar su razón teleológica y cambiar estructuralmente los Servicios de Inteligencia estatales; es decir, enmarcar sus actividades dentro del sistema legal, jurídico y democrático. Según el *Acuerdo sobre Fortalecimiento del Poder Civil y Función del Ejército en una Sociedad Democrática*, «18. La seguridad es un concepto amplio que no se limita a la protección contra las amenazas armadas externas, a cargo del Ejército, o a la protección contra las amenazas al orden público y la seguridad interna, a cargo de la Policía Nacional Civil. El conjunto de los Acuerdos de Paz de Guatemala plantea que la paz firme y duradera requiere el respeto a los derechos humanos, y al carácter multiétnico, pluricultural y multilingüe de la Nación guatemalteca, el desarrollo económico del país con justicia social, la participación social, la conciliación de intereses y el fortalecimiento de la institucionalidad democrática.

»19. Dentro de este concepto, la seguridad ciudadana y la seguridad del Estado son inseparables del pleno ejercicio por los ciudadanos de sus derechos y deberes políticos, económicos, sociales y culturales. Los desequilibrios sociales y

¹⁰⁵ *Constitución Política de la República de Guatemala*, Artículo 1º.

¹⁰⁶ *Constitución Política de la República de Guatemala*, Artículo 2º.

económicos, la pobreza y la pobreza extrema, la discriminación social y política, la corrupción, entre otros, constituyen factores de riesgo y amenazas directas para la convivencia democrática, la paz social y, por ende, el orden constitucional democrático.»

En el mismo acuerdo se establece (del numeral 36 al 52), que los Organismos de Inteligencia del Estado deberán readecuarse a las exigencias propias de un Estado Democrático y se recomiendan las características que deberán tener a partir de que se firme la paz.

Con esa visión y tomando en cuenta, fundamentalmente, el espíritu de los demás *Acuerdos de Paz*, la *Constitución Política de la República de Guatemala*, el *Tratado Marco de Seguridad Democrática en Centroamérica* y la *Ley Marco del Sistema Nacional de Seguridad*, se diseñó la *Política Nacional de Seguridad* (2012). Esta recogió todos esos instrumentos de concordia y legales para conducir sus actos en la consecución de la seguridad ciudadana.

Todo lo anterior, naturalmente, exigió la creación de un Sistema Nacional de Seguridad, definido en la *Ley Marco del Sistema Nacional de Seguridad*, que agrupara a todas las instituciones cuyas actividades eran relativas a la seguridad ciudadana.¹⁰⁷ Las actividades del Sistema Nacional de Seguridad se normaron

¹⁰⁷ Según esta ley, «El Sistema Nacional de Seguridad está integrado por:

- »a) Presidencia de la República;
- »b) Ministerio de Relaciones Exteriores;
- »c) Ministerio de Gobernación;
- »d) Ministerio de la Defensa Nacional;
- »e) Procuraduría General de la Nación;
- »f) Coordinadora Nacional para la Reducción de Desastres —CONRED0—;
- »g) Secretaría de Inteligencia Estratégica del Estado —SIE—; y,
- »h) Secretaría de Asuntos Administrativos y Seguridad de la Presidencia de la República —SAAS—.»

también en la *Ley Marco del Sistema Nacional de Seguridad*. Allí también se definió el Sistema Nacional de Inteligencia y sus componentes.¹⁰⁸

¹⁰⁸ **ARTÍCULO 24.** «Sistema Nacional de Inteligencia. El Sistema Nacional de Inteligencia es el conjunto de instituciones, procedimientos y normas que abordan con carácter preventivo, las amenazas y riesgos a la seguridad de la Nación, mediante la necesaria coordinación de las funciones de Inteligencia estratégica, civil y militar, así como de cada una de ellas en su ámbito de actuación.

»Es responsable de producir Inteligencia y conducir la Contrainteligencia, trasladándola a las respectivas autoridades superiores, de conformidad con las atribuciones asignadas por la presente ley y demás disposiciones pertinentes.

»Está integrado por la Secretaría de Inteligencia Estratégica de Estado, quien lo coordina, la Dirección de Inteligencia Civil del Ministerio de Gobernación, la Dirección de Inteligencia del Estado Mayor de la Defensa Nacional del Ministerio de la Defensa Nacional.

»Todas las instituciones del Organismo Ejecutivo deberán proporcionar a la Secretaría de Inteligencia Estratégica de Estado la información que ésta les requiera sobre los asuntos de su competencia.

Capítulo III

1. La denuncia

1.1 Concepto

Una de las acepciones del verbo «denunciar», que da el *Diccionario de la Real Academia Española*, es: «Dar a la autoridad judicial o administrativa parte o noticia de una actuación ilícita o de un suceso irregular.»¹⁰⁹ El cuerpo de una denuncia en Guatemala, según el artículo 299 del *Código Procesal Penal* establece que debe contener: «en lo posible, el relato circunstanciado del hecho, con indicación de los partícipes, agraviados y testigos, elementos de prueba y antecedentes o consecuencias conocidos.»

En las denuncias hay dos aspectos:

1. Que todo ciudadano puede hacer las denuncias sobre una presunta falta o delito.

2. Que muchos ciudadanos se abstienen de hacer las respectivas denuncias por:

A. Falta de confianza en el sistema para darle seguimiento a la denuncia.

B. Miedo a las represalias.

C. Desconocimiento del proceso para hacer una denuncia, etc.

¹⁰⁹ Consultado en: <http://buscon.rae.es/drae/srv/search?id=tzITHnA3VDXX2CqKdE95>, el 18 de julio de 2014, a la 9:100 horas.

Por tales razones, se deben hacer esfuerzos institucionales para que la población adquiriera una cultura de denuncia; por modernizar y agilizar un sistema de denuncias que sea eficaz y le dé confianza a la ciudadanía.

El concepto moderno de denunciar ha evolucionado a través del tiempo, como sucede con buena parte de las palabras de un idioma, para encontrar un sentido más adecuado entre lo que se piensa y la mejor manera de expresar lo pensado. En el Derecho Romano, por ejemplo, que es de donde arranca este concepto jurídico, se usaba para requerir a un vecino que no realizara una obra en un terreno ya que, al hacerlo, afectaría los intereses del denunciante. Este terreno podía ser público o privado. A este acto se le denominaba *operis novi nuntiatio* (o.n.n.), que puede traducirse como denuncia de obra nueva y peligrosa.

1.2. Por qué es importante denunciar

El objeto de las denuncias, en términos generales, es poner en conocimiento de las autoridades la comisión de ilícitos, faltas o delitos para que estas se encarguen de darle seguimiento; que la víctima reciba alivio, compensación, resarcimiento o protección ante las amenazas que puedan derivarse del hecho denunciado. Denunciar es hacer uso del derecho que le asiste a una persona de invocar el deber del Estado contenido en el artículo 2º. de la *Constitución Política de la República de Guatemala* que consiste en «garantizarle a los habitantes de la República la vida, la libertad, la justicia, la seguridad, la paz y el desarrollo integral de la persona.»

1.3. ¿Qué implica una cultura de denuncia?

Implica que las personas tengan conciencia de la importancia de denunciar lo ilícito y los delitos a las autoridades; esto, con el ánimo de lograr un mejor espacio para la convivencia. Si se hace una denuncia es porque se tiene la confianza o, por lo menos, la esperanza de que el delito:

- a) Será investigado.
- b) Será castigado el infractor o infractora.
- c) Se contribuirá a evitar la impunidad.
- d) Contribuirá a disuadir a quienes quieran delinquir.
- e) El Estado de Derecho se fortalecerá. etc.

2. ¿Se puede mejorar el sistema de denuncia automatizando digitalmente los procesos?

La posibilidad para que tal mejora pueda darse resulta casi obvia en tanto que, en primer lugar, supone una actualización tecnológica (que sí es posible) en todos de los centros de acopio de información concernientes a la seguridad nacional; no obstante, ese cambio tecnológico, también implica un cambio de mentalidad en quienes son los operadores de tal acopio y, por supuesto, su propia tecnificación y capacitación. El cambio de mentalidad, para aceptar el reemplazo de una tecnología por otra, siempre fue un elemento importante en el avance o estancamiento de un proceso. Este es un aspecto que se da no solo en lo individual o en pequeños grupos sino, también, en sociedades o naciones. Un ejemplo de esta falta de adaptación nos lo da Manuel Castells, en su libro *La Era*

de la Información (Pág. 26), al decirnos que en la raíz del derrumbamiento de la Unión Soviética «se encuentra la incapacidad del estatismo para gestionar la transición a la era de la información.» Eso implicó no solo un estancamiento sino que, con el avance de los años implicó un retraso tecnológico que hasta muchos años después comenzó a recuperar, ya no como Unión Soviética sino como Federación Rusa.

En el caso de Guatemala, ese mismo temor al cambio ha implicado que, aun hoy, todavía se utilicen tecnologías desfasadas en muchas instancias gubernamentales, lo cual provoca ineficiencia y lentitud burocrática. Lo dijo Otto Pérez Molina, al recalcar «la resistencia a los cambios, principalmente dentro del propio Gobierno.»¹¹⁰ A pesar de lo anterior, la misma demanda de Seguridad ha motivado que las autoridades encargadas de la seguridad ciudadana hayan reparado en esta deficiencia y comiencen a estar anuentes a la modernización del sistema de acopio de denuncias. El Ministerio de Gobernación anunció, en agosto de 2013, la creación de un nuevo Sistema de Información Policial (SIPOL), que permitirá «registrar en línea las denuncias por diferentes delitos, faltas y otros hechos de interés policial, facilitando al ciudadano estar menos tiempo dedicado a una denuncia, así como poder tramitarlo al momento de acudir a las comisarías donde los agentes encargados usarán esta plataforma virtual enviándolas a donde corresponde para iniciar con las pesquisas. El plan piloto se inició con la capacitación de los efectivos asignados en la comisaría 14. [Pero el problema

¹¹⁰ Secretaría Técnica del Consejo Nacional de Seguridad, *Política Nacional de Seguridad*, Guatemala, 2012, Pág. V.

sigue siendo que esa información estará concentrada en la PNC, sin que se adscriba al SNS].

»Además este Sistema de Información Policial, SIPOL, estará disponible en los dispositivos móviles que porten los agentes de la PNC, pues ellos podrán recibir las denuncias desde el lugar de donde se registró el hecho, así lo explicó Juan Carlos Argueta, Viceministro de Tecnología y Comunicaciones del Ministerio de Gobernación: “es un sistema web que estamos utilizando que permite ingresar denuncias desde los dispositivos móviles como *tablets* y teléfonos inteligentes, ello permite acercarse al ciudadano”.»¹¹¹

El ejemplo anterior es un indicio de que sí es posible la mejora en este aspecto pero también de que en materia de denuncias, todas las instituciones deben coordinarse para que la información pueda generarse de manera fluida, rápida y exacta.

Hay otro caso, en el Ministerio Público, que se dio con el ánimo de facilitar la denuncia respecto a casos de las extorsiones: la habilitación del teléfono número 2411-911. La noticia apareció el 10 de julio de 2014, en el portal del Ministerio Público, y dice: «La iniciativa surge para brindar una atención directa y especializada a favor de la población que es víctima de hechos extorsivos, informo en conferencia de prensa el jefe de la Fiscalía contra el Crimen Organizado, Lic. Ronny López, quien se hizo acompañar del fiscal encargado de la Unidad contra las Extorsiones, Lic. Raúl Figueroa.

¹¹¹ Página web del Ministerio de Gobernación: http://www.mingob.gob.gt/index.php?option=com_k2&view=item&id=4425:pnc-implementa-nuevo-sistema-para-denuncias&Itemid=103

»El licenciado López señaló que el número telefónico habilitado funcionará las 24 horas. Cada denuncia será recibida por personal calificado y capacitado, además la Fiscalía dará seguimiento a la investigación de cada caso denunciado.»¹¹²

Los esfuerzos, tanto de la PNC, como del MP son encomiables; sin embargo parecen condenados al fracaso porque, según pude comprobar, prácticamente ninguna de las personas (de distintos estratos sociales) a quienes pregunté, estaban enterados de la existencia de esos sistemas de denuncia. En el caso del Ministerio Público, el sistema de denuncias por medio del teléfono debería abarcar no solo las relacionadas con la extorsión sino con todo tipo de delitos o faltas. Pero fundamentalmente debería, en primer lugar, concebirse una campaña masiva por todas las instituciones involucradas con la seguridad pública y ciudadana para dar a conocer sus sistemas de denuncias y las maneras de acceder a ellos. Si no se comienza por eso, cualquier sistema de denuncias que se implemente constituirá un esfuerzo vano por mejorar el sistema de justicia en Guatemala.

Una campaña para promover una cultura de denuncia debería comenzar por hacerle saber al ciudadano las distintas instancias públicas a las que puede acudir para plantear una denuncia; además, indicar los medios de los cuales se puede servir para plantearla: oral y escrita. En lo oral, por medios telefónicos, de manera directa, por medio de otras personas, etc. En lo escrito, por la denuncia en papel o por medios electrónicos. También será importante que se le explique a qué

¹¹² Página web del Ministerio Público: <http://www.mp.gob.gt/2014/07/ministerio-publico-habilita-el-numero-2411-9119-para-recibir-denuncias-de-extorsion/>

institución debe acudir el ciudadano para cada caso de delito o falta que esté dispuesto a denunciar. Actuar de manera rápida y eficaz para que el ciudadano comience a tener confianza en el sistema de denuncias y no siga desentendiéndose de él por considerarlo una pérdida de tiempo. Este aspecto es de suma importancia; en la actualidad, con voluntad política y combatiendo a la vez la corrupción, puede optimizarse sobre todo automatizando, modernizando digitalmente y unificando, el sistema de denuncias que llegue a cada una de las instancias del SNS.

3. Modernización de la tecnología de acopio de denuncias

Modernizar implica actualizar; la idea es servirse de la tecnología para lograr un servicio de Inteligencia que sea más eficiente en la producción de información. En consecuencia, más efectivo en la dotación de seguridad a todos los ciudadanos guatemaltecos. En la medida en que el Estado no se actualice, corre el riesgo de ser más vulnerable ante las amenazas cada vez más sofisticadas y tecnificadas que se ciernen sobre él y la sociedad. Por eso se debe evitar el rezago tecnológico y mantener una permanente actualización tecnológica en la dotación de la seguridad ciudadana que además es una de las principales razones teleológicas del Estado de Guatemala y tiene carácter constitucional.

La actualización no solo es necesaria sino fundamental para que el Estado tenga ventaja y pueda anticiparse a las amenazas que se ciernen sobre él. La actualización siempre será de carácter constante porque su vigencia es limitada, ya que en el mercado siempre surgirán opciones más avanzadas con mejores expectativas de eficacia. Esa acción del mercado, dura mientras las fuerzas que

atentan contra la seguridad ciudadana y estatal logran rebasar las diferencias o ventajas del sistema estratégico del Estado. «La tecnología tiene una curva de desarrollo que se inicia con un gran impulso, cuando las pruebas experimentales de la tecnología de que se trate demuestran que existe una solución funcional para el problema en cuestión. En un segundo momento, crecen las expectativas sobre esa solución para entrar en un periodo de ajuste en el que esas expectativas se contextualizan en su justa dimensión y, finalmente, ocurre un descenso que se conoce como la parte de la *curva de la decepción*, donde se ubica el nicho exacto en que tiene cabida la nueva solución.

»Una vez que la nueva tecnología llega hasta el nicho que le corresponde, experimenta un desarrollo real y sostenido, sin sobresaltos; crece de forma moderada y sostenida hasta alcanzar su plenitud para finalmente entrar en un declive en su etapa de obsolescencia, lo que da paso a una nueva tecnología.»¹¹³

3.1. Virtudes en las implementaciones de base de datos

La descentralización es un aspecto que incide en la eficiencia de las instituciones del Estado; contribuye reemplazar el centralismo y autoritarismo que lo afectó hasta tiempos recientes y a tener más en cuenta los intereses mayoritarios y el involucramiento de la sociedad en las decisiones políticas y administrativas. En el ámbito de la Seguridad, las tareas para ese objetivo recaen en el Sistema Nacional de Seguridad; sin embargo, por la naturaleza de la información que se maneja, se necesita de cierta discrecionalidad; no se puede relegar al

¹¹³ Reyes Bravo, Raymundo, en: Herrera-Lasso Mijares, Luis (Responsable), ESISEN, *Tecnología para los Servicios de Inteligencia*, México, 2010, Pág. 28.

conocimiento público indiscriminado y su manejo solo debe darse en el ámbito institucional. No obstante, «estará sujeta a controles democráticos».¹¹⁴ Por tal razón y para cumplir con las nuevas razones teleológicas del Estado, en un ámbito democrático, las funciones de seguridad, información e Inteligencia estatal, se concentraron en el Sistema Nacional de Seguridad, creado a partir de la *Ley Marco del Sistema Nacional de Seguridad*, como se estipula en el Artículo 1 de la citada ley: se establecen «las normas jurídicas de carácter orgánico y funcional necesarias para la realización coordinada de las actividades de seguridad interior, exterior y de Inteligencia por parte del Estado de Guatemala, para que en forma integrada, sistematizada, eficiente y eficaz esté en capacidad de anticipar y dar respuesta efectiva a riesgos, amenazas y vulnerabilidades, a fin de estar preparado para prevenirlos, enfrentarlos y contrarrestarlos en observancia de la Constitución Política de la República, el respeto de los derechos humanos y el cumplimiento de los tratados internacionales ratificados por Guatemala.» En tal virtud, «Un servicio de Inteligencia debe tener una infraestructura capaz de: recopilar, enviar, procesar, almacenar, proteger y gestionar la información empleada para producir Inteligencia.»¹¹⁵

3.2. Qué es una base de datos

En términos generales una base de datos es un conjunto de datos reunidos en algún medio o soporte. Este medio, en consecuencia, es una especie de almacén

¹¹⁴ *Ley Marco del Sistema Nacional de Seguridad*, Artículo 3.

¹¹⁵ Gutiérrez Zarazúa, Gerardo en: Herrera-Lasso Mijares, Luis (Responsable), ESISEN, *Tecnología para los Servicios de Inteligencia*, México, 2010, Pág. 14.

donde, de manera organizada y relacionada entre sí, se guardan datos. Por ejemplo, un diccionario es una base de datos en la que, en orden alfabético, se ordenan los datos que están constituidos por las «entradas» y sus respectivas acepciones. No obstante, el término abarcó las más diversas formas de almacenamiento, como ficheros, kárdex, tablas, etc. Las bases de datos comenzaron a tener relevancia en el ámbito informático, a partir de la década de los años 60, del siglo pasado. Con el avance de la informática, los soportes sobre los cuales se concentraban las bases de datos fueron mejorando su capacidad de almacenamiento, disponibilidad y uso. Además de los llamados discos duros, se utilizaron como soportes discos flexibles; luego llegaron los discos compactos (CD, por sus iniciales en inglés), las Intranet, la Internet, memorias externas, servidores, memorias USB y ahora se ha vuelto común la utilización de las nubes públicas o privadas que permiten la Internet y las Intranet. En resumen, la tecnología y los modernos *hardware* y *software* han mejorado de manera ostensible la capacidad de las bases de datos.

3.2.1. Para qué sirve una base de datos

Las bases de datos sirven, básicamente, para almacenar datos e información de la más diversa índole; para que los datos e información puedan almacenarse según la jerarquía más propia y acorde con los intereses y objetivos a los que van a servir, y puedan convertirse en información; consultarse sin que implique la aparatosa burocracia, esfuerzo e incomodidad que antes requería examinar enormes volúmenes de páginas, archivos o fichas en grandes ficheros que hacían

lento cualquier proceso de almacenamiento y proveeduría de datos e información. Las bases de datos modernas pueden ser administradas por diversos sistemas; para el tema de la investigación que nos ocupa, las bases de datos serán administradas por un *data center* también llamado *datawarehouse* programado con tecnologías específicas de *hardware*, *software* de aplicación especial que tendrá todas las características que el SNS demande para la captación de denuncias, tecnologías de almacenamiento y comunicaciones. «Los *data warehouse*¹¹⁶ “corren” un sofisticado software de base de datos que es el que organiza y administra realmente los datos.»¹¹⁷ Una base de datos adecuada a la captación de denuncias en un sistema unificado como el del SNS, tendrá la ventaja de que permitirá tomar mejores decisiones; en el ámbito de la investigación constituirá un insumo valioso para la Inteligencia Estratégica del Estado de Guatemala y para todas las instituciones que agrupa el SNS de Guatemala.

Una base de datos que reúna y unifique las captaciones de denuncias de las distintas instituciones agrupadas en el SNS, facilitará, entre otras funciones:

- Aumentar la capacidad investigativa en los diversos aspectos de la seguridad interna y externa del Estado y la ciudadanía.

¹¹⁶ En el capítulo I, inciso 1., en pie de página, se explicó en qué consiste un *datawarehouse* (o almacén de datos), término que en textos y en la jerga informática se utiliza alternativamente como *datacenter*.

¹¹⁷ Dyché, Jill, *E-data*, Prentice Hall, Arge tina, 2001, Pág. 49.

- Compartir de manera rápida la información y, en consecuencia, agilizar la investigación para, de esa manera, proveer mejores insumos en la impartición de justicia.

- Proporcionar una visión que centralice las características fundamentales de los sujetos delictivos.

- Monitorear de mejor manera la investigación de los hechos delictivos para, después, poder predecirlos y anticiparse a su suceso.

- Mejorar la capacidad de respuesta, de acuerdo con las responsabilidades de las diversas instituciones que conforman el SNS.

- Contribuir de mejor manera al registro estadístico de los hechos delincuenciales y sus efectos colaterales.

- Aumentar y mejorar la credibilidad de las instituciones encargadas de la seguridad ciudadana.

3.2.3. Tipos de bases de datos

Según los usos y objetivos de las bases de datos existe la más variada diversidad; sin embargo, las más usadas o en las que la mayoría se sustenta, son dos:

A. Bases estáticas.

B. Bases dinámicas.

Las bases estáticas almacenan datos que, una vez ingresados, serán inmodificables; en general, son de carácter histórico; es decir se van produciendo a través del tiempo; por ejemplo las que almacenan cronologías, expedientes médicos, estadísticas, etc. Los usos principales que se dan a este tipo de base de

datos consisten en deducir información de ellas para la realización de proyecciones, análisis y toma de decisiones.

Las bases de datos dinámicas guardan datos que con el transcurso del tiempo pueden modificarse, ampliarse, actualizarse, borrarse, etc. Dentro de estas bases, las más usadas son las llamadas bases de datos relacionales.

Una base de datos relacional consiste en relacionar los datos para producir información. Por ejemplo, si se trata de una persona que delinquirió, con una base de datos de esta naturaleza, puede establecerse qué tipo de delito cometió, en dónde, con quién, a quién, etc.

«Los inicios de las base de datos modernas se deben sobre todo al desarrollo realizado por el inglés Edgar Frank Codd, que propuso el primer modelo teórico relacional, es decir, definió cómo se debían relacionar los datos pertenecientes a una base de datos. Por otro lado, IBM desarrolló la primera definición de lenguaje para base de datos (que definía cómo añadir y extraer información de una base de datos) llamado SEQUEL. Más tarde SEQUEL acabaría convirtiéndose en el lenguaje más utilizado hoy en día con bases de datos, el SQL.

»SQL se ha convertido en un lenguaje estándar para todas las bases de datos. Hoy día es empleado por prácticamente todas las bases de datos existentes. Como en todo lenguaje ha habido mejoras y por tanto nuevas versiones a lo largo del tiempo, pero aunque cada sistema de base de datos tenga

sus propias particularidades, todos comparten muchas características comunes.»¹¹⁸

3.2.3. La base de datos para las denuncias

El acopio de denuncias, ya sean orales o escritas, por la variedad y naturaleza de cada una de las que puede darse, requiere de personal capacitado para recibirlas, de una base de datos que además de ordenarlas, provea de una guía o formato que facilite la recepción y su respectivo procesamiento para que luego pueda ser fuente útil para convertirse en información; en consecuencia, pueda analizarse y facilite o permita tomar las decisiones más adecuadas. La base de datos debe estar dotada de la mayor seguridad posible para que sea confiable y sirva de apoyo institucional para generar confianza en la ciudadanía.

No todas las denuncias pueden ser sujetos de investigación o de resguardo en una base de datos. En primer lugar, la denuncia debe tratarse de hechos o circunstancias que puedan ser calificadas como faltas o delitos. Que el supuesto infractor sea plenamente identificado y que los operadores de justicia constaten que se trata de faltas o delitos que están incluidas en el Código Penal o que no haya prescrito el tiempo para presentar la denuncia. Más adelante, detallaré en detalle la estructura de la base de datos para las denuncias. No obstante, una base de datos de denuncia, en general, debe integrar los siguientes elementos:

¹¹⁸ Sierra, Manuel, en: http://www.aprenderaprogramar.com/index.php?option=com_attachments&task=download&id=500 consultado el 15-9-2014, a las 10:00 horas.

3.2.3.1. Introducción. En esta parte se incluirá el nombre del denunciante, fecha de presentación de la denuncia, la dirección para recibir notificaciones.

3.2.3.2. Hechos denunciados. Esta sección estará constituida por la descripción del delito o falta denunciada; se incluirán las circunstancias en las cuales se dio y entre quienes. Para facilidad de análisis, seguimiento e investigación, cada elemento de lo denunciado se enumerará, ya sea con números ordinales o con las letras del alfabeto; por ejemplo:

A. El señor X agredió de manera violenta y verbal a su esposa.

B. Lo hizo de manera pública.

C. Le provocó dos hematomas; una en el pómulo izquierdo y otra en el pómulo derecho.

4. Etcétera.

3.2.3.3 Causas del asunto. Explicación del origen de la denuncia.

3.2.3.4 Medios de investigación. Detalle de los indicios o evidencias que se presentan para validar la denuncia.

3.2.3.5. Petición del denunciante. Inclusión de la solicitud de la persona denunciante, ya se trate de solicitar medidas cautelares u otras medidas de seguridad.

3.2.4. Estructura de una base de datos

La estructura de una base de datos para el acopio de denuncias, aunque tiene elementos comunes con otras bases de datos, deberá diseñarse y funcionar de la manera más adecuada en función de los objetivos para los cuales se creará. En tal sentido debe tener en cuenta, como mínimo, los siguientes elementos:

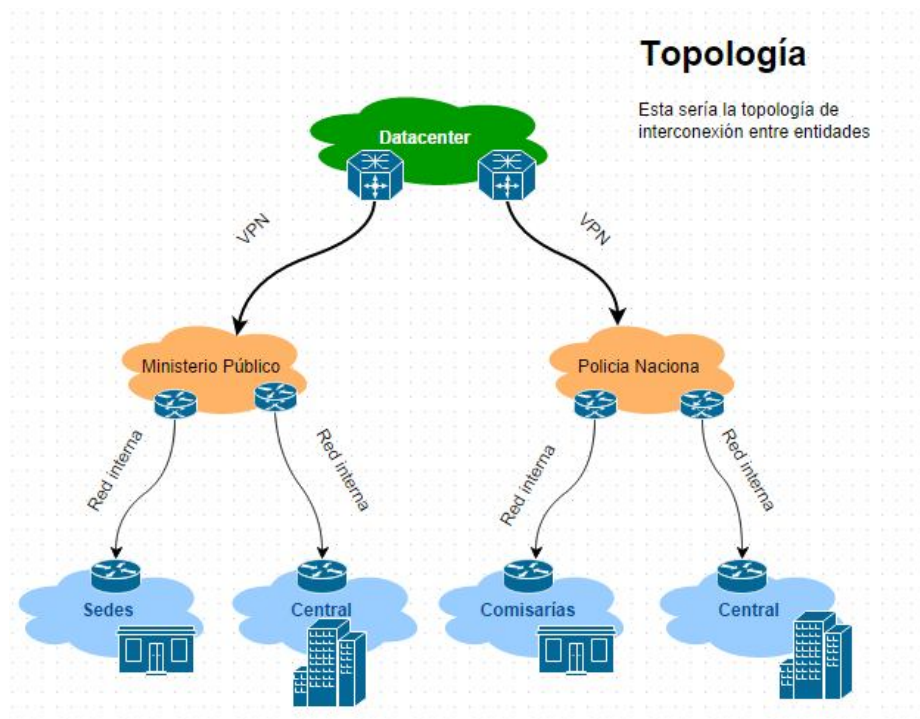
1. Que permita el registro de las denuncias que se presenten y que sea, como se dice en el ambiente informático, «amigable».

2. Que permita que el denunciante pueda acudir a los lugares habilitados institucionalmente para hacerla y que encuentre receptores de la denuncia que le faciliten el trámite.

3. Que la denuncia presentada por el denunciante genere un código que identifique la denuncia y que en el SNS la clasifique de manera única.

El marco legal para la generación de una base de datos para la captación de denuncias, tiene su fundamento legal en el Artículo 2, inciso h) de la *Ley Marco del Sistema Nacional de Seguridad*, al definir el Ciclo de Inteligencia y especificar, dentro del conjunto de actividades que lo componen, «planificar, identificar información, recolectar, procesar, analizar, producir, distribuir y difundir información de manera oportuna, para la toma de decisiones al más alto nivel del Sistema Nacional de Seguridad.»

Las especificaciones técnicas de una base de datos para la captación de denuncias dentro de un Sistema Unificado y adscrito al SNS, debe contar con un *hardware* y un *software* que formarán parte de un *datacenter*, que presenten las características mínimas que se requieren para el caso y funcionen adecuadamente en cada una de las terminales de acopio, procesamiento, distribución entre los investigadores y para el análisis de denuncias. La topología de ese sistema puede graficarse de la siguiente manera (del SNS solo se incluyen al Ministerio Público y la Policía Nacional Civil, para mejor visualización):



VPN: Red privada virtual, por sus siglas en Inglés: *Virtual private network*.

3.2.5. Equipo

A continuación describo el equipo necesario para el funcionamiento adecuado de un sistema de denuncias del SNS. Lo descrito está pensado para un plan piloto a ejecutarse en el departamento de Guatemala:

- **Equipo de almacenamiento:** SAN Hitachi Data Systems HUS 110
 - 100 TB utilizables, aprox 70% con discos SAS 600GB 10K RPM, aprox 30% con discos SAS 1.2TB 10K RPM, ambos en RAID 5.

Este tipo de equipo de almacenamiento es adecuado pensando en unas 100 mil denuncias mensuales y que con este volumen, se llene en aproximadamente 4 años. No obstante, el sistema permite la compra de más memoria para ir expandiendo su capacidad.

- **Servidores:**

- 2 Blade Server Enclosure, No Blades, M1000E

- 6 Servidores Blades Dell M520 (Opción 2)

- 4 Swtich Brocade M5424 FC8 Switch + AG, 24 ports with 4 8Gb SFPs,

Redundant Configuration

- 4 Swtich PowerConnect M6348, 48 GbE Ports, Managed Switch, 10GbE

and Stacking Capable, Redundant

- 1 RACK APC

Este sistema está diseñado con “redundancia”; esto quiere decir que si se «cae» el servicio de un servidor, entra a funcionar el otro; lo cual permite que el funcionamiento nunca se descontinúe.

- **Firewall.** El *Firewall* sirve para crear el VPN (protocolo virtual). Para crear un canal seguro entre los sistemas UPS; es decir, para que solo las personas autorizadas puedan acceder a él mediante protocolos, contraseñas y otras medidas de seguridad.

- FortiGate 800C. Rendimiento de firewall de 20 Gbps y rendimiento IPS de 6 Gbps y 10-GbE interfaces en un factor de forma 1U. FortiGate-800C es un componente adecuado para utilizarlo en las comunicaciones seguras entre las distintas instituciones del SNS.

- UPS: Sistema De alimentación ininterrumpida, por sus siglas en inglés: *uninterruptible power supply*.

- APC Smart-UPS RT 5000VA 208V w/ 208V to 120V Step-Down Transformer. Sirve para mantener el voltaje estable de los servidores.

- **Software:** SAP for Defense & Security.

La solución SAP for Defense & Security ofrece información de recursos en tiempo real, de modo que personal-comando y control pueden determinar continuamente el estado de disponibilidad operacional. Con este *software* se puede planificar mejor y prestar apoyo desplegado de operaciones mediante el uso de una gama de funciones de planificación integrada de todos los recursos, incluidos los recursos humanos, material, infraestructura y finanzas. SAP for Defense & Security permite evaluar exhaustivamente los costos y actividades; también, presentar nuevas opciones para la colaboración y el intercambio de datos entre instituciones. La solución ofrece una visibilidad total de los recursos, desde la fábrica hasta la trinchera, y viceversa, por lo que el personal de servicio siempre conoce los activos que están en el almacenamiento, en tránsito y en proceso. Puede asignar más fácilmente sus activos en contra de sus pasivos, lo que resulta en una planificación más eficiente y precisa. SAP for Defense & Security ayuda a aumentar el porcentaje del presupuesto que se asigna a las misiones operativas en lugar de la logística y administración, lo que permite optimizar recursos financieros. Se puede hacer la solución interoperable e integrarla horizontalmente con los sistemas militares, proporcionando así información de múltiples fuentes y ayudar al personal a tomar las decisiones correctas en situaciones críticas. SAP for Defense & Security es impulsado por la plataforma SAP NetWeaver, lo que significa que el usuario puede realizar la mayor parte de las funciones existentes mediante el uso de servicios de la institución, la protección de la información, y reducir el costo total de funcionamiento.

La cartera de soluciones contiene los siguientes componentes de software específicos de la industria y ha sido desarrollado en colaboración con el Grupo de Interés de Defensa (Deig):

El (DFPS) componente Defensa y Fuerzas de Seguridad Pública es parte de SAP ERP y ERP; ofrece funciones específicas para la defensa y la seguridad pública.

SAP Mobile Defense & Security (SAP MDS) permite el uso en línea y fuera de línea de los procesos de defensa seleccionados. Funcionalidades móviles permiten el mantenimiento móvil, gestión de materiales móviles, y la organización móvil y dotación de personal.

SAP Military Data Exchange (SAP MDE) proporciona capacidades off-the-shelf gestión vigor que permiten la interoperabilidad con los Sistemas de Mando y Control de la Información (CCIS) y la OTAN Funcionales Área de Servicios (FAS).

- **Licencias de Virtualización.** 20 licencias VMware vSphere with Operations Management.

- *Router.* Router Cisco. Permite la comunicación de rutas para redes internas o externas

- *Enlaces.* Enlaces con cada institución, dedicados a mantener la vinculación y el flujo de la información.

- *Scanners:* Cada centro de acopio de denuncias estará provista con un scanner, para poder copiar facsimilarmente las denuncias que se lleven escritas. Existen en el mercado muchas opciones; sin embargo una práctica podría ser la

impresora Canon multifuncional Pixma MP250, que además de impresora tiene funciones de fotocopidora y de scanner.

3.2.6. Funcionamiento

La función principal de un sistema unificado de denuncias, dentro del SNS, es contribuir a proveer información para la seguridad estratégica ciudadana y estatal de los guatemaltecos. En este sentido, la denuncia constituye una de las actividades principales que hacen funcionar el Ciclo de Inteligencia que, como ya especifiqué en el Capítulo I de esta investigación, para el caso de Guatemala, está definido en el Capítulo II, inciso h), de la *Ley Marco del Sistema Nacional de Seguridad*.

Ante el crecimiento poblacional que se da con el paso de los años, la denuncia se ha hecho fundamental para aumentar la capacidad investigativa del Estado. Los aparatos de Inteligencia estratégica estatales, por sí solos, serían incapaces de obtener la información necesaria sobre todos los ilícitos que se cometen o perpetran en un territorio. Por eso es fundamental el involucramiento ciudadano; por la misma seguridad ciudadana y para alimentar el sistema democrático en el que la ciudadanía debe involucrarse en todas las instancias estatales para sentirse parte de él; sobre todo, para que su aporte contribuya a su propia seguridad. La denuncia es fundamental; por tal razón, ante las necesidades de información que el Estado requiere satisfacer, sobre todo en los últimos tiempos, que las mismas instituciones estatales se han visto en la necesidad de fomentarla por medio de los más diversos recursos. Un ejemplo de esa urgencia

de denuncia se vio, por ejemplo en el ámbito norteamericano, con el ofrecimiento de recompensas ofrecidas por el gobierno mexicano y el estadounidense por información que llevara a la captura de Héctor Beltrán Leyva: «Las autoridades estadounidenses ofrecían una recompensa de 5 millones de dólares por información que llevara a su captura, y las mexicanas de 30 millones de pesos (unos 2.2 millones de dólares).»¹¹⁹ Dentro del ámbito guatemalteco, la recompensa por la denuncia del paradero de Waldemar Lorenzana: «La justicia norteamericana ofrecía US\$500 mil de recompensa por información vital que permitiera la captura de Lorenzana.»¹²⁰ Éste, finalmente fue capturado el 26 de abril de 2011.

Por tal razón para un efectivo funcionamiento de un sistema unificado de denuncias dentro del SNS, sobre todo en la captación, la base de datos instalada debe ofrecer la posibilidad de que el ingreso de la información sea una operación sencilla y que, a la vez, los usuarios estén capacitados para su mejor manejo. También que la denuncia contenga los elementos fundamentales, según se enumeró en apartado 3.1.4. Para eso se hace necesario el uso de plantillas, en línea, que evitarán la improvisación y asegurarán que sean consignados los datos necesarios para la eficacia de la denuncia.

Los requerimientos técnicos, además del *Hardware* y demás elementos consignados en el apartado 3.1.5 deben «cumplir con los requisitos básicos

¹¹⁹ Mark Stevenson y E. Eduardo Castillo, | Associated Press, tomado de: <https://es-us.noticias.yahoo.com/beltr-n-leyva-se-ocultaba-plena-vista-en-195629547.html>, el 3-10-2014, a las 10:24 horas.

¹²⁰ *Prensa Libre*, 26 de abril de 2011.

expresados por el triángulo de la seguridad, es decir, que promuevan la confidencialidad, la integridad y la disponibilidad de la infraestructura y desde luego, de la información.»¹²¹ Además, tener como mínimo, las especificaciones siguientes:

- Un sistema operativo (por ejemplo, Windows 7).
- Internet, ya sea que se use el buscador Internet Explorer o el Google Chrome en sus versiones actualizadas.

- Acrobat Reader en su versión actualizada.
- Winrar 3.62 o versión actualizada.
- Win Zip 7.0 o versión actualizada.
- Office en versión actualizada.

En el sistema operativo de denuncias, para facilitar su operación, se incluirá un menú de captura de denuncias en cuya plantilla se incluirán, como mínimo, las pestañas siguientes:

- **Información general**, en la que de manera sucinta, se describirá la naturaleza de la denuncia. Al hacer clic en esta casilla, se desplegarán los elementos requeridos de la denuncia:

- **No. de denuncia**. Este será el código único con el cual se identificará en todo el SNS la denuncia presentada. Con este código las personas interesadas podrán darle seguimiento a la denuncia.

¹²¹ Reyes Bravo, Raymundo, en: Herrera-Lasso Mijares, Luis (Responsable), ESISEN, *Tecnología para los Servicios de Inteligencia*, México, 2010, Pág. 24.

- **Lugar donde se presenta la denuncia.** Puede ser una oficina del Ministerio Público, de la Policía Nacional Civil o de cualquier otra agencia de las instituciones del SNS.

- **Fecha de presentación.**

- **Hechos denunciados.** En esta sección se detallan los hechos denunciados.

- **Solicitud de la persona denunciante.** Aquí se especificará la solicitud del denunciante, ya se trate de medidas cautelares u otras medidas judiciales.

- **Denuncia escaneada.** En el caso que la persona denunciante haya llevado por escrito su denuncia, se escaneará. En tal circunstancia, a la par se pondrá la opción «si», o «no».

- **Denunciantes.** Aquí se especificará el nombre de la persona denunciante.

En esta pestaña se incluirán los datos siguientes:

- **Tipo de denuncia.** En este apartado se especificará si la denuncia es sobre robo, asesinato, secuestro, etc.

- **Nombre.** Se especificará el nombre completo de la persona denunciante.

- **Dirección.** Aquí se consignará la dirección exacta del domicilio de la persona denunciante, salvo que se trate de una denuncia anónima.

- **Teléfono.** En esta casilla se consignará el número telefónico de la persona denunciante, salvo que se trate de una denuncia anónima.

- **Denunciados.** Aquí se especificará el nombre de la persona o personas denunciadas.

- **Tipo de denuncia.** En este apartado se especificará si la denuncia es sobre robo, asesinato, secuestro, etc.

- **Nombre.** Se especificará el nombre completo de la persona denunciada.
- **Dirección.** En esta casilla se anotará la dirección exacta de la persona denunciada, o en su defecto un ámbito geográfico en el que pueda ser localizado.
- **Teléfono.** De ser posible se consignará el número telefónico de la persona denunciada.
- **Anexos.** En esta pestaña se incluirán, si fuera el caso, documentos presentados, pruebas, etc.

Este sistema de denuncias también se hará extensivo para que, en línea, los ciudadanos puedan ejercer su derecho a denunciar ilícitos.

4. Procesos obsoletos de las denuncias actuales

Un proceso, tecnológicamente, puede ser muy moderno y actualizado, pero si no es usado de la manera más adecuada implica una inversión o esfuerzo sub utilizado. Sería como regalarle un avión moderno a un niño de 4 años y que este no pueda utilizarlo porque, en primer lugar, no sabe leer; en segundo no sabe pilotar un avión; en tercero, no tenga la edad requerida para pilotarlo. Se vería bonito en su hangar, pero no cumpliría las funciones para las que tal artefacto fue creado. Del mismo modo, a la vez que es necesario modernizar o actualizar de manera permanente los equipos y las capacidades técnicas, es preciso que los usuarios estén compenetrados a fondo de las virtudes del sistema y capacitados para hacer que estos sean eficaces. A la vez, se puede contar con el mejor equipo, el personal mejor capacitado, pero si los ciudadanos no acuden a denunciar, también la inversión y el esfuerzo se verán sub utilizados. Por tal razón,

como ya explicaré en el apartado 9 de este capítulo III, es necesario y urgente que el Estado fomente una cultura de denuncia entre la población.

4.1. Crítica al sistema de denuncias del Ministerio Público

«El Ministerio Público es una institución con funciones autónomas, promueve la persecución penal y dirige la investigación de los delitos de acción pública; además velar por el estricto cumplimiento de las leyes del país. En el ejercicio de esa función, el Ministerio Público perseguirá la realización de la justicia, y actuará con objetividad, imparcialidad y con apego al principio de legalidad, en los términos que la ley establece.»¹²²

Según el portal del Ministerio Público (MP), para presentar una denuncia se necesita:

«- Documento de identificación personal.

»- Aportar información relacionada con el hecho, con indicación de los partícipes, agraviados y testigos, elementos de prueba y antecedentes o consecuencias conocidos.»¹²³

Lo que no se dice en el Portal del MP ni en la *Ley Orgánica del Ministerio Público*, es el procedimiento para realizar tal denuncia y cómo se procesará. Al no establecerse con claridad el sistema de denuncias, el denunciante no puede tener certeza absoluta de que su denuncia será procesada. Por otra parte, al no estar incluido el Fiscal General dentro del Consejo Nacional de Seguridad, según se advierte en el Artículo 9 de la *Ley Marco del Sistema Nacional de Seguridad*,

¹²² Congreso de la República de Guatemala, *Ley Orgánica del Ministerio Público*, Artículo 1.

¹²³ <http://www.mp.gob.gt/preguntas-frecuentes/>

desvincula al Ministerio Público de la obtención fluida y directa que se genere dentro del SNS, lo cual me parece incongruente; también la burocratiza, aunque la *Ley Orgánica del Ministerio Público*, en su Artículo 6, lo faculta para «pedir la colaboración de cualquier funcionario y autoridad administrativa de los organismos del Estado y de sus entidades descentralizadas, autónomas o semiautónomas, para el cumplimiento de sus funciones, estando éstos obligados a prestarla sin demora y proporcionar los documentos e informes que les sean requeridos.

»Las autoridades, los funcionarios y los organismos requeridos por el Ministerio Público, en ejercicio de las facultades que le otorga la ley, deberán atender inexcusablemente el requerimiento dentro de los límites legales y el término establecido en el requerimiento.»

4.2. Crítica al sistema de denuncias de la Policía Nacional Civil

Si bien la PNC cuenta ahora con el SIPOL, como ya se explicó arriba, la información se centraliza en la PNC y no en el SNS. Esto implica que cualquiera de las instituciones del SNS que requiera información de la PNC, debe obtenerla por medio de un proceso que implica burocracia, lentitud en la obtención de la información y, por tanto, ineficacia o lentitud en el actuar de las demás instituciones del SNS. Por otro lado, La utilización del sistema es del conocimiento solo de una minoría de la población, lo cual también le resta eficacia.

5. Codificación de seguridad para el resguardo de la información para que solo las instituciones designadas y el personal autorizado puedan tener acceso a la información

Casi todos los ámbitos del actuar humano conllevan precauciones que inciden en su realización segura; por ejemplo, si uno va a la calle y observa que el cielo está nublado, llevará paraguas, por si llegara a llover; si regresará tarde, llevará abrigo para protegerse del frío, etc. De la misma manera, para el resguardo de la información deberán observarse ciertas precauciones. Los sistemas de resguardo de la información cambiaron drásticamente en pocos años debido, fundamentalmente, a los avances tecnológicos; de lo manual se pasó a lo automático y, de allí, a lo digital. Muchos de los conceptos sobre seguridad tecnológica, en la actualidad, «se orientan a eliminar, mitigar, transferir o aceptar los riesgos y vulnerabilidades que los mismos avances tecnológicos implican.»¹²⁴

La seguridad debe enfocarse no solo en correctivos para problemas que ya sucedieron sino, también por medio del análisis de todas las posibilidades de amenaza o riesgo que pudieran darse en el futuro dentro del SNS.

«Una estrategia integral de seguridad tecnológica debe considerar:

- »• La definición de una política de seguridad.
- »• La evaluación de riesgos que enfrente la institución de que se trate.
- »• Definir claramente las tareas y responsables de la seguridad tecnológica.

¹²⁴ Villegas Lastra, Raúl A., en: Herrera-Lasso Mijares, Luis (Responsable), ESISEN, *Tecnología para los Servicios de Inteligencia*, México, 2010, Pág. 55.

»• La sensibilización y formación del personal en los asuntos correspondientes a la seguridad.

»Las mejores prácticas indican que todos los puntos que se deben considerar para una estrategia integral de seguridad son importantes. Los esfuerzos deben tener el siguiente orden de prioridades: procedimentales, formativos y, finalmente, tecnológicos.»¹²⁵

Para un sistema de denuncias unificado, como el que se plantea en esta investigación es necesaria una seguridad tecnológica que incluya, como sugiere Raúl A. Villegas Lastra (Págs. 57-58), los siguientes servicios: confidencialidad, autenticación, integridad, no repudio,¹²⁶ disponibilidad. Con excepción de la disponibilidad, que no puede garantizarse de manera absoluta, ya que existe la probabilidad de fallas en el sistema debido a fallas técnicas, a fenómenos naturales o de otra índole. Todos los demás servicios es posible garantizarlos mediante distintas herramientas.

Cada Estado tiene sus propios requerimientos de seguridad para el resguardo de su información; por ejemplo, en muchos países el enfoque está concentrado en el terrorismo; en otros en el narcotráfico, la trata de personas, etc. En Guatemala están especificados en el capítulo IV de la *Política Nacional de Seguridad*.

¹²⁵ Ídem, Págs. 55-56

¹²⁶ «... garantiza que una entidad involucrada en la comunicación no pueda repudiar una acción realizada. Por ejemplo, permite validar que un usuario envió un correo electrónico, incluso cuando en un momento dado éste lo niegue.» (Villegas Lastra, Raúl A., en: Herrera-Lasso Mijares, Luis [Responsable], ESISEN, *Tecnología para los Servicios de Inteligencia*, México, 2010, Pág. 58).

Como la transmisión de la información se hará básicamente por medio de la Internet o de la Intranet, es preciso extremar las medidas de seguridad en el resguardo de la información. Por eso, como ya se detalló en el apartado 3.1.6, la instalación de un *Firewall*, será el filtro primario que impedirá que personas o equipos no autorizados puedan tener acceso a la información. Por tal razón, se privilegiará el uso de la Intranet como medio más adecuado para la transmisión o envío de la información crítica. La red privada, o Intranet, en Guatemala por el momento tiene dos posibilidades; una, el arrendamiento de una red que se considera segura y que la única empresa que la ofrece es Movistar. La otra es construyendo la red de manera enteramente privada, lo cual tiene un costo considerablemente superior al arrendamiento, pero se considera la más segura. Esto implicaría el tendido de una red de fibra óptica que entrelazaría a todas las instituciones del SNS. Este tipo de red, por supuesto, no determina la seguridad total de la información, pero constituye una primera dificultad para que personas ajenas, no autorizadas, puedan acceder a la información.

Un elemento importante en la seguridad y resguardo de la información es la dotación de códigos de usuario a cada persona que se le autorice la entrada a la base de datos; de tal manera que a la hora de un análisis forense digital sea posible identificar al usuario que accedió a la base de datos, el día y la hora en que lo hizo, la información que ingresó o utilizó, la autorización jerárquica que lo llevó a ingresar a la base, para qué le servirá la información y, en fin, otros indicios que aseguren que la información no se fugará o caerá en manos inadecuadas o que harán mal uso de ella.

Otro elemento para el resguardo de la información es la encriptación, que básicamente consiste en un sistema de signos que a ojos de una persona ajena o desconocedora de los códigos usados, no podrá informarle de nada. Los métodos de encriptación son diversos. Cada institución, de acuerdo con sus necesidades o posibilidades, determina el más adecuado.

Pero la seguridad no está delimitada solo al uso indebido de la información: también tiene que ver con ataques dirigidos de manera directa o indirecta contra las bases de datos. Los directos pueden darse por medio del sabotaje, ciberterrorismo, suplantación de identidad, etc. Los indirectos, sobre todo se dan con los llamados «virus informáticos».

Es sabido que los virus informáticos aparecieron por primera vez en 1983, cuando el profesor de informática Len Adleman observó que un alumno suyo se apoderó de un ordenador con un sencillo programa; en ese momento tuvo la certeza que se trataba de un virus, pero digital. En la actualidad, así como los avances tecnológicos han dado un gran salto, las amenazas también han crecido casi en la misma proporción. Cada año se renuevan los antivirus respondiendo a nuevas amenazas; sin embargo eso no es una garantía completa porque se han dado bastantes casos en los que los antivirus han sido inoperantes porque la sofisticación del virus no permitió su identificación oportuna. En ese sentido se ha hecho muy necesaria una especie de higiene digital que impida el ingreso de los virus informáticos. Los virus se generan por millones, así que pensar que un antivirus hace inmune a una base de datos es falso. Luego vinieron los ataques directos a las bases de datos con el fin de destruirlos o dañarlos. En la actualidad,

quién no ha escuchado sobre los hackers, cuya denominación, en general, designa a delincuentes informáticos. En Guatemala han ocurrido sinnúmero de ataques de hackers, por ejemplo a portales de distintas instituciones como el Congreso de la República, según informó *Prensa libre* el 16 de agosto de 2011; o, según informó el mismo diario, el 25 de marzo de 2012, la incursión en la página web del Arzobispado de Guatemala, con ocasión de la visita a México del papa Benedicto XVI.

Por las razones anteriores y muchas no mencionadas, es preciso que no se escatimen los esfuerzos para que el resguardo de la información sea confiable y seguro; por tal razón es imprescindible codificar y encriptar la información que se resguarde para que solo las instituciones designadas y el personal autorizado puedan tener acceso a ella.

Por supuesto, algo que es fundamental en el manejo de la información que se recabe en el Sistema de Denuncias del SNS es la confidencialidad, que está normada en el artículo 76 del *Reglamento de la Ley Marco del Sistema Nacional de Seguridad*: «Los miembros, funcionarios empleados y asesores que conforman el Sistema Nacional de Inteligencia tienen, estrictamente prohibido, dar a conocer, suministrar información o permitir el acceso a los expedientes, documentos, notas, informaciones o material de cualquier tipo que, por razón de sus funciones, sea de su conocimiento.»

6. Integración del Sistema de Denuncias de todas las instituciones estatales vinculadas con el Sistema Nacional de Seguridad

A lo largo de esta investigación he demostrado la importancia de integrar en un solo Sistema de Denuncias los sistemas particulares de cada institución del SNS.

Las ventajas más visibles de ese proceso son las siguientes:

- Eliminación de protocolos burocráticos que retardan la provisión de la información.

- Posibilidad de darles mejor seguimiento a las denuncias.

- La integración del sistema de denuncias permitirá la elaboración de un protocolo con enfoque victimológico para darles un tratamiento adecuado a las víctimas y, de esa manera, el daño ocasionado en ellas no se acentúe. Este protocolo también contribuirá a la prevención victimal o prevención victimológica.

- Al estar en disposición de dar una mejor respuesta a lo denunciado, será posible que la población cuente con un elemento para recuperar la confianza en las autoridades, sobre todo, respecto a la seguridad ciudadana. De paso se contribuirá a que la justicia aspire a ser pronta y cumplida.

Solo con esas ventajas, si se consigue la unificación, se habrá dado un gran paso en el camino hacia el logro de una sociedad más justa y armónica.

7. Creación de un Reglamento y Código Ético que deberán regir el uso de la información generada por este sistema unificado de información

El SNS es de reciente creación y producto de un proceso que devino, en buena medida, de los *Acuerdos de Paz*. No obstante que se establecieron los objetivos, medios y maneras de hacer eficaz y perfectible el Sistema, no se dotó de un instrumento o código ético que estableciera los principios conductuales que deberán conducir el actuar del personal que lo integraría. Aunque el *Reglamento de la Ley Marco del Sistema Nacional de Seguridad* especifica las reglas generales que han de tenerse en cuenta en la ejecución de la ley, a la postre la conducta ética que deberán observar los integrantes del Sistema es discrecional. En la *Ley Marco del Sistema Nacional de Seguridad*, tan solo el artículo 25 establece una prohibición de carácter ético y en el *Reglamento de la Ley Marco del sistema Nacional de Seguridad*, solo el artículo 76. Así que ese vacío es importante llenarlo para que el SNS y, específicamente, el Sistema de Denuncias del SNS encuadre de mejor manera en un Estado democrático.

8. Capacitación y tecnificación del personal encargado de recibir las denuncias

Tal como lo indica el artículo 15 de la *Ley Marco del Sistema Nacional de Seguridad*, «Las instituciones que forman el Sistema Nacional de Seguridad están obligadas a establecer programas de profesionalización en su respectiva

especialidad.» Esta normativa obedece al mismo principio de actualización del que se habló arriba. No resulta lógico que el equipo y demás instrumentos del SNS se modernicen si los operadores y empleados no se actualizan. En el caso de quienes reciben las denuncias, su función no solo consiste en recibirlas sino en saber guardarlas de mejor manera para que su utilidad sea óptima; además, y de manera fundamental, en tratar de la mejor manera a quienes acuden a denunciar, para que se sientan en confianza y la denuncia pueda ser eficaz; tendrán que poseer una formación mínima en aspectos legales referidos, sobre todo, a la denuncia y conocer todos los mecanismos y canales para que las denuncias surtan el efecto de iniciadores de un proceso legal y, además, alimenten el Sistema de Inteligencia del Estado.

9. Campaña nacional de educación para el acceso al sistema de denuncias

¿Para qué una campaña nacional para el acceso al sistema de denuncias? Para que los ciudadanos puedan tener acceso a este Sistema de Denuncias y hacer el uso más adecuado de él; además, dentro de esta campaña, fortalecer la cultura de denuncia en todos los ciudadanos. Como todo en la vida, el Sistema irá perfeccionándose en la práctica; sin embargo, dar este paso es fundamental para mejorar esta parte inicial de los procesos judiciales y, en consecuencia, contribuir a que la justicia sea pronta y cumplida.

10. Concepto de una denuncia a nivel social

En la búsqueda de la justicia, el ser humano se ha servido de los más diversos recursos para conseguirla. Denunciar la injusticia ha sido uno de los medios más eficaces pero no siempre el camino más fácil ni la oportunidad que todos han tenido. La denuncia individual a veces carece de efectividad porque el esfuerzo es aislado. La denuncia social por el contrario, ha demostrado a través de la historia una efectividad más contundente, aunque tampoco implica garantía total. Este tipo de denuncia se ha practicado de las más diversas maneras. Una de las más importantes, y quizá pionera en las demás formas de ejercerla, es la manifestación social. No obstante, hacerla efectiva es complejo porque implica organización, recursos estratégicos, logística y otros factores, además de, en la actualidad, legalizarla; no obstante, la fuerza con que se la reprimía antes ha disminuido en violencia y la actual modalidad democrática permite, en muchos casos, que se pueda ejercer de manera más libre. Y, siempre, a los que están a favor, se les contrapondrán los que están en contra. Ejemplos de esa situación se dan a menudo en la actualidad. Luego, un tipo de denuncia social que ha dado muestras de eficacia es la que se hace a través de los medios de comunicación y los medios masivos que se dan en las redes sociales. La importancia de esas denuncias sociales que se dan en la actualidad es su notoriedad y, en consecuencia, la facilidad con la que pueden llegar a las instancias de poder o decisión. También, ahora el Ministerio Público puede actuar, de oficio, cuando se trate de denuncias

sociales de delitos; y, con la gestión de esta entidad, llevar la denuncia a su proceso normal.

11. Cifra negra de la criminalidad

La modernización de la tecnología también es importante para poder estimar de mejor manera la cifra negra que, en Criminología, consiste en el desconocimiento de los delitos o delincuentes por no haber sido denunciados o descubiertos por el sistema judicial o investigativo de un país. «... los estudios disponibles (PNUD 2007, ODHAG 2011 y este mismo) apuntan a una tendencia en que más de dos terceras partes de los hechos de violencia no llegan a denunciarse en ninguna institución.»¹²⁷

Los investigadores chilenos Benavente y Cortés sostienen que en la mayoría de los estudios sobre la criminalidad en el mundo «se asume que el nivel de denuncias está directamente relacionado con el nivel efectivo de criminalidad que existe en la sociedad». Pero respecto a lo último advierte: «Existen fundadas sospechas y argumentos de que esto no es así. En primer lugar, la cifra negra de delitos, es decir, la diferencia entre los delitos efectivamente acontecidos y las denuncias asociadas a éstos, puede no ser nula; ello debido a la existencia de elementos que impidan o desincentiven a la víctima a realizar la denuncia correspondiente. Estos elementos podrían estar relacionados con las características socioeconómicas de la víctima y/o a la percepción que ésta tenga

¹²⁷ Oficina de Derechos Humanos del Arzobispado de Guatemala, *Violencia en Guatemala*, Guatemala, 2013, Pág. 6.

acerca de la eficacia y eficiencia del sistema jurídico- policial que le rodea.» El autor chileno agrega: «En segundo lugar, existe evidencia – aunque aún muy preliminar de que efectivamente el nivel de denuncias puede aumentar en el tiempo sin estar necesariamente asociado a un incremento real en el nivel de delitos. Este fenómeno de subreporte puede, en consecuencia, generar distorsiones no solo en los determinantes de la criminalidad sino también en las implicancias de política que puedan, a partir de esta información, derivarse».¹²⁸

En este punto, es primordial advertir que las iniciativas que se promuevan para mejorar el nivel de confianza en las víctimas para que presenten sus denuncias, si bien incrementarían la cantidad de denuncias se debe comprobar empíricamente que esto contribuirá a disminuir el número de delitos. Habría que establecer el impacto que tendrían las cifras de subreporte vinculadas con los delitos y la clase de ilícitos de que se trate. Podría ocurrir, al contrario, que la estabilidad del nivel de denuncias en el tiempo más bien oculte el recrudecimiento los niveles de criminalidad en la sociedad y que éste se reporta de manera efectiva, debido a los obstáculos y costos que existen en el sistema jurídico-policial. No obstante, ante la carencia de datos, no se pueden separar los motivos de los delincuentes para perpetrar sus acciones de las características de las víctimas para que tengan la confianza de presentar las denuncias. Esto implica que es crucial separar las características de las víctimas de las de los victimarios,

¹²⁸ Benavente, José Miguel y Enrique Cortés. *Delitos y sus denuncias. La cifra negra de la criminalidad en Chile y sus determinantes*, Universidad de Chile, Facultad de Economía y Negocios, Serie Documentos de Trabajo, No. 228, Santiago, 2006. Disponible en <https://www.academia.edu/4147235/Delitos_y_sus_denuncias._La_cifra_negra_de_la_criminalidad_en_Chile_y_sus_determinantes>. Consultado el 21 de febrero de 2016.

así como del medio que los rodea. Las características personales de quienes hacen las denuncias no corresponden, necesariamente, con las de quienes son los victimarios. Esto implica que las razones que tiene la víctima al tomar la decisión de denunciar no tienen por qué coincidir con los móviles del victimario al materializar su comportamiento delictivo.

12. Encuestas de victimización

Un aspecto muy importante, también, dentro de la modernización tecnológica es la sistematización de las encuestas de victimización, «que consisten en un cuestionario realizado a un grupo representativo de la población, acerca de su calidad de víctima de un delito determinado, índice que arroja los delitos acontecidos, su frecuencia y las características de la gente victimizada. Se refieren a la relación de la víctima con el procedimiento penal. Esto con el objeto de elaborar propuestas de política criminal tanto preventiva como represiva.»¹²⁹

13. La inversión

Un estimado de la inversión mínima, necesaria para la adquisición del equipo e infraestructura de un sistema unificado de denuncias, dentro del SNS, se especifica a continuación:

Almacenamiento:

¹²⁹ Olgún Rojas, Karina, citada en: González Guzmán, Carlos Fernando, *La situación de las víctimas en la legislación nacional Derivada de las Reformas al Decreto 57-92 del Congreso de la República*, Guatemala, 2012, Pág. 12.

SAN Hitachi Data Systems HUS 110 - 100 TB utilizables, aprox 70% con discos SAS 600GB 10K RPM, aprox 30% con discos SAS 1.2TB 10K RPM, ambos en RAID 5	\$.150,000.00
---	---------------

Servidores:

Descripción	Cantidad	Precio
Blade Server Enclosure, No Blades, M1000E	2	\$. 20,000.00
Servidores Blades Dell M520 Opción 2	6	\$. 48,000.00
Switich Brocade M5424 FC8 Switch + AG, 24 ports with 4 8Gb SFPs, Redundant Configuration	4	\$. 44,000.00
Switich PowerConnect M6348, 48 GbE Ports, Managed Switch, 10GbE and Stacking Capable, Redundant	4	\$. 12,000.00
RACK APC	1	\$. 2,000.00
Total		\$. 126,000.00

Firewall:

FortiGate 800C Rendimiento de firewall de 20 Gbps y rendimiento IPS de 6 Gbps y 10-GbE interfaces en un factor de forma	\$. 45,000.00
--	---------------

1U, FortiGate-800C es ideal para empresas medianas y grandes sucursales de la empresa	
---	--

UPS:

APC Smart-UPS RT 5000VA 208V w/ 208V to 120V Step-Down Transformer	\$. 10,000.00
--	----------------

Software:

SAP for Defense & Security	\$. 400,000.00
----------------------------	-----------------

Licencias de virtualización:

VMware vSphere with Operations Management 20 licencias	\$. 90,000.00
---	----------------

Router:

Router Cisco	\$. 25,000.00
--------------	----------------

Enlaces:

Enlaces a cada entidad	\$. 2,000.00
------------------------	---------------

Capítulo IV

1. Internet, desobediencia civil y legítima resistencia del pueblo

1.1. De la «Primavera árabe» a la «Primavera guatemalteca»

A fines de 2010 y principios de 2011, el mundo árabe fue convulsionado por la “revolución Twitter” y la “revolución Facebook”. Los dictadores en Túnez y Egipto fueron defenestrados por los movimientos “online” que se combinaron con las manifestaciones “fuera de línea”. Al igual que en la denominada “Primavera Árabe”, la Internet también se convirtió en un espacio de confrontación social en Guatemala con las movilizaciones que, de abril a septiembre de 2015, forzaron las renuncias del Presidente y de la Vicepresidenta de la República.

En los tres casos, *Facebook* y *Twitter* fueron la caja de resonancia de la indignación contra los abusos de poder y la corrupción. Las redes sociales transmitieron y amplificaron las frustraciones ciudadanas, así como las reivindicaciones de quienes recurrieron tanto a la desobediencia civil como a la legítima resistencia del pueblo. En Túnez y Egipto la censura no logró evitar que el resto del mundo siguiera en directo los acontecimientos, en los que hubo derramamiento de sangre. En contraste, en Guatemala no se registró ningún incidente violento durante casi cinco meses de protestas. Los teléfonos móviles desempeñaron una función crucial. Los ciudadanos convertidos en periodistas, nutrieron con imágenes los sitios donde se comparten fotografías, videos, así como los sitios de *streaming*.

En Túnez y Egipto las autoridades trataron infructuosamente de imponer el silencio mediático sobre los acontecimientos. En cambio, en Guatemala los gobernantes no lograron reaccionar frente a las presiones incontenibles en el ciberespacio. En nuestro país, los canales de televisión abierta perdieron su influencia sobre el sistema dominado por los partidos políticos. Los medios televisivos propiedad del magnate mexicano Ángel González, fueron remplazados, en su rol de fuentes y vectores de la información, por las redes sociales y los sitios web informativos. *Facebook* funcionó como plataforma para que los internautas enviaran regularmente comentarios y todo tipo de imágenes.

La Internet ha convocado masas para derrocar gobiernos que antes no creyeron que podían ser atacados por otros medios. El dictador libio, Muhammar Gadafi le preguntó a Ben Alí cuando iniciaron las protestas en Túnez: «¿Vamos a convertirnos en víctimas de Facebook y Youtube?».¹³⁰ El interrogante que no ocultaba cierto escepticismo, después adquirió un cariz providencial. Días después, los ciudadanos derrocaron a Alí. Por primera vez en la historia del mundo árabe, los indignados salieron a las calles, convocados por las redes sociales. La pregunta de Gadafi se transformó en un postulado. El descontento popular encontró un catalizador que cobró su primera víctima.¹³¹

Convocados por medio y a través de la Internet, los grandes protagonistas de las convulsiones en Túnez, Egipto y Guatemala fueron movimientos ciudadanos

¹³⁰ Águila, Isaías Acata. "Internet, un derecho humano de cuarta generación." *Misión Jurídica: Revista de derecho y ciencias sociales*, Vol. 4, No. 4, 2011, Págs. 37-58. Disponible en <<https://dialnet.unirioja.es/servlet/articulo?codigo=5167589>>. Consultado el 20 de febrero de 2016.

¹³¹ *Ibíd.*

espontáneos. En Guatemala, la denominada “sociedad civil” no abanderó la toma de plazas y calles. Este fenómeno no ha sido estudiado, al igual que los derechos, las libertades y las garantías que se vinculan con las nuevas tecnologías de la información. Hoy puede afirmarse que la Internet se transformó en un derecho humano de la cuarta generación: «Cuando los medios de comunicación, los sindicatos, y el poder judicial y político están sojuzgados por el poder omnívoro de los dictadores, está ahora Internet como el instrumento más eficaz para convocar a la sublevación. La libertad de expresión encuentra su mejor aliado en la World Wide Web o RED, entrando en escena el triunvirato de las protestas: Twitter, Facebook y YouTube».

La Internet se transformó en lo puede denominarse «tecno-poder». La red propicia que los valores sociales se encarnen en la vida diaria, por medio de la tecnología. Detrás de esa tecnología se ocultan cuestiones políticas, sociales e ideológicas de dimensiones inimaginables. La Internet está en la médula de los asuntos geopolíticos. Esto se debe, en parte, al hecho de que en el ciberespacio no puede soslayarse la infraestructura que sustenta a la red, por lo que para esta tesis resulta primordial reflexionar acerca del papel del Estado en la creación de las redes, su configuración, y el tipo y la nacionalidad de los operadores. Aparte, la Internet se ha constituido en un ámbito en la cual confluyen los retos políticos y estratégicos. Esta circunstancia impone al Estado la obligación de mantenerse vigilante frente a las nuevas amenazas contra la Seguridad de la Nación, y por ende, que puedan perjudicar la vida, la integridad física y psicológica, y los bienes de las personas.

Los casos de desobediencia y resistencia en Túnez, Egipto y Guatemala pusieron en evidencia que la *Web* se convirtió en un campo de batalla. La Internet se ha constituido en un importante catalizador de las inconformidades civiles. Las comunidades virtuales se erigieron como nuevas instancias que recurren a la Internet para ir más allá de las consignas políticas. Se ha construido un nuevo terreno de enfrentamiento político entre los sistemas políticos y sus oponentes.

En este nuevo espacio virtual-real, el Estado puede bloquear la Internet, pero solo lo logrará por medio del autoritarismo. En Túnez, el «techo-control» lo ejercían los familiares de Ben Alí. En Egipto, por los familiares de Mubarak y los militares. En Guatemala, no había control alguno y menos regulaciones a las que se pudiera recurrir. Históricamente, como veremos a continuación, la desobediencia civil surgió frente a disposiciones gubernamentales consideradas ilegítimas, aunque estuvieran arropadas por la legalidad. No necesariamente se ha canalizado por la vía pacífica. En cambio, la legítima resistencia del pueblo es pacífica por naturaleza. El pueblo solo puede reaccionar con fuerza cuando el Estado lo ataca con violencia. En nuestro país, esa es su esencia, al tenor del artículo 45 de la Constitución Política de la República.

En Túnez, el régimen de Ben Alí no intentó bloquear la Internet ya que consideraba que lo vital para el sistema era crear una base de datos de información personal de los usuarios que actuaban políticamente. Esa estrategia se basó en el empleo de «cookies» y «puertas traseras» (Backdoors), para obtener las contraseñas de los usuarios y activistas. El propósito era acceder a sus cuentas y comprobar sus buzones, creando una «lista negra» de los

sediciosos que serían interrogados más tarde. Sin embargo, el régimen subestimó las dimensiones de los acontecimientos y el inmenso impacto de la Internet, así como de sus modos de cifrado y la capacidad de anonimato. Empresas como *Google*, *Facebook* o *Twitter* desarrollaron soluciones técnicas para impedir el acceso a sus sistemas. De esa manera se anuló la estrategia del régimen, y lo capitanearon hacia la imposibilidad de actuar, inmovilización que era muy difícil de superar.¹³²

En Egipto, la situación era más compleja. Se trató del levantamiento popular más divulgado en la historia de las sublevaciones. Los servicios de inteligencia gubernamentales no accedieron a los contenidos de los intercambios virtuales, sino interrumpieron la conexión a la Internet durante cinco días. Ante el precedente de Túnez, el régimen egipcio cayó en la cuenta de que no era posible reaccionar y superar el reto de la «guerra virtual» contra las revueltas, debido al vértigo de la información que se generaba, así como frente al excesivo número de activistas virtuales políticos, empoderados para precipitar los acontecimientos y de generalizar la opinión popular para derrocar al régimen. Con esa decisión de «cortar» la Internet, el régimen de Hosni Mubarak perpetró, según el diario *Libération* del 28 de febrero de 2011, «el acto más dictatorial de la historia sobre el derecho de acceso a la información que nunca se ha cometido, ni siquiera por Birmania en 2007, China en 2008, o Irán en 2009, para convertirse en el enemigo

¹³² Disponible en <<http://www.rsf-es.org/grandes-citas/dia-contra-censura-en-internet/a2011-dia-mundial-contra-la-censura-en-internet/frente-a-la-censura-solidaridad-en-la-red/>>. Consultado el 20 de febrero de 2016.

número uno de Internet, según Reporteros sin Fronteras». ¹³³ Esa estrategia no podía resistir por mucho tiempo a causa de que los operadores de telecomunicaciones aplicaron medidas para desviar del tráfico de la Internet, como una solución para evitar el control que pretendía ejercer el régimen egipcio sobre la red. Fue así como *Google Oriente Medio*, para sortear la censura implantada por el régimen, posibilitó el envío de mensajes a Twitter desde el teléfono móvil. Además, *French Data Network* (FDN), una asociación de militantes por el derecho de acceso a Internet, brindó acceso a los servicios *Web* a partir de sus plataformas y aplicaciones virtuales. ¹³⁴

En Guatemala, la crisis política iniciada en abril de 2015 demostró que las redes sociales –fundamentalmente *Facebook* y *Twitter*- se consolidaron como vehículos para que la información circulara de manera rápida y sin censura. También demostraron su efectividad cuando se convocaron las movilizaciones sociales. Cada uno de los hitos de la toma de conciencia ciudadana podía medirse en *Twitter* y comprobar la relevancia de las redes sociales como herramientas políticas.

De acuerdo con datos confirmados por la consultora en transformación digital *Findasense*, para la primera manifestación fijada para el 25 de abril de 2015, por medio de *Facebook* se enviaron 66,000 invitaciones. Se logró convocar a 15,000 personas, que se congregaron para exigir la renuncia de la entonces

¹³³ El Hamdouni, Youssef. "Internet y la primavera árabe: hacia una nueva percepción del ciberespacio." *Paix et sécurité internationales: revue maroco-espagnole de droit international et relations internationales* 1 (2013): 167-173. Disponible en <<https://dialnet.unirioja.es/servlet/articulo?codigo=4580274>>. Consultado 20 de febrero de 2016.

¹³⁴ *Ibidem*.

vicepresidenta Roxana Baldetti, manifestándose por medio del *hashtag* #RenunciaYa.¹³⁵

Cuatro meses después, la negativa del presidente Otto Pérez Molina de renunciar provocó la convocatoria al paro nacional del 27 de agosto. Ese fue el día con mayor interacción en redes sociales del año en Guatemala. Del total de conversaciones, 69% de las mismas fueron generadas por hombres en *Twitter* y 31% por mujeres. Alrededor de 100,000 personas se reunieron en la Plaza de la Constitución y recurrieron a sus redes sociales para generar casi 98,000 conversaciones, el récord de conversaciones en el año.¹³⁶

El 1 de septiembre de 2015, 132 diputados al Congreso aprobaron retirar la inmunidad del presidente Otto Pérez, después de los señalamientos del Ministerio Público (MP) y la Comisión Internacional Contra la Impunidad en Guatemala (CICIG) de ser el «cabecilla» de una estructura de defraudación tributaria. Minutos después, miles de usuarios de redes sociales manifestaron su apoyo a la decisión de los parlamentarios. En la red social *Twitter* una de las etiquetas que los usuarios compartieron fue #ExijoMis105Votos. La misma etiqueta sirvió para que las personas expresaran su júbilo por la histórica votación del Congreso. Además de la mencionada etiqueta, otra que rápidamente se posicionó en la lista de favoritas de esa red social fue #1SEPGT. Finalmente, Otto Pérez Molina renunció el miércoles 2 de septiembre.¹³⁷

¹³⁵ Disponible en <<http://www.estrategiaynegocios.net/tecnologia/876092-330/redes-sociales-protagonistas-de-la-crisis-en-guatemala>>. Consultado 20 de febrero de 2016.

¹³⁶ *Ibíd.*

¹³⁷ Disponible en <<http://www.prensalibre.com/guatemala/comunitario/retiro-de-inmunidad-de-perez-molina-incendia-redes-sociales>>. Consultado 20 de febrero de 2016.

El lunes 25 y martes 26 de enero, Pérez Molina concedió entrevistas divulgadas por la cadena alemana para el extranjero *Deutsche Welle* (DW) y por el diario español *El Mundo*, respectivamente. En su encuentro con la cadena alemana, Pérez Molina afirmó: «nosotros sabemos que a través de la embajada y con dinero de Estados Unidos se movieron las redes sociales para incentivar la participación de la población», refiriéndose a las manifestaciones ciudadanas que empezaron el 25 de abril de 2015 y prosiguieron de manera ininterrumpida durante 19 semanas. Agregó: «mucha gente actuó inocentemente y creyendo, pero lo que estaba detrás moviendo todo esto habían unos intereses, unos propósitos y una articulación que estaban haciendo muy claramente. El resultado de toda esta articulación fue que mucha gente decidiera asistir al Parque Central, pero mucha gente que llegaba con cientos de peticiones. Pero algunos medios de comunicación se han levantado de que fue el pueblo que se levantó completamente. Yo gané con casi dos millones y medio de votos. Y la manifestación más grande si mucho llegó a 80 mil personas. Dicen que fue espontáneo y que la población salió, pero aquí hubo mucha manipulación también», afirmó a DW. Sobre el mismo asunto, el ex gobernante afirmó a *El Mundo*: «Yo digo que aquí no ha existido la ‘primavera’ guatemalteca».¹³⁸

La participación ciudadana es uno de los elementos fundamentales dentro de un sistema democrático; sirve de manera esencial para equilibrar el poder en la relación Estado-sociedad. La democracia no existiría sin la participación

¹³⁸ Disponible en <<http://www.prensalibre.com/guatemala/politica/perez-molina-no-he-cometido-ningun-delito>>. Consultado el 20 de febrero de 2016.

ciudadana: a mayor participación ciudadana, más se fortalece y consolida la democracia. La democracia, aunque no es un sistema perfecto, es perfectible.

Los Estados latinoamericanos, sobre todo a partir de la década de los noventa del siglo pasado, han dado un vuelco en los sistemas políticos prevalecientes y se han inclinado por la democracia. Esto incluye a Guatemala. La democracia, para perfeccionarse necesita, ante todo que se ejercite; ese ejercicio en buena medida es resultado de la educación que comienza desde la familia y se prolonga en la escuela, en la universidad y en prácticamente todas las instancias de la vida. Es un sistema en el cual se privilegia el consenso y el diálogo en oposición a la imposición.

La justificación teleológica del Estado, en el caso de nuestro país, está establecida en la *Constitución Política de la República de Guatemala*, cuando establece, en el artículo 1º., que «su fin supremo es la realización del bien común.» En tal sentido, el Estado está en función de la sociedad y no, como en sistemas políticos anteriores, que la sociedad estaba en función del Estado, del rey, de príncipes o de otros poderes.

La desconfianza que la ciudadanía, en general, tiene sobre la ineficacia de la denuncia tiene sus raíces en la poca credibilidad que tiene en las instituciones estatales. Los motivos para esa desconfianza la ciudadanía los observa a diario. Basta hojear las páginas de los diarios para enterarse sobre la intervención de un organismo de Estado en el campo de acción de otro, sobre la intervención e influencia de poderes extra estatales para influir en decisiones que vulneran el Estado de Derecho; sobre las promesas que los candidatos políticos hacen en sus

campañas y el incumplimiento de las mismas al asumir el poder, etc. La lista es larga. Entonces, si los actores institucionales no generan confianza, las instituciones se debilitan y pierden efectividad para cumplir con los objetivos establecidos en las leyes y los fundados en la democracia. Esa es, entre muchas, una de las justificaciones para la desobediencia civil o para la legítima resistencia del pueblo, derivada de que la ley se vuelve injusta al no ser observada por quienes debieran dar el ejemplo en su cumplimiento. Y también de que quienes tienen a su cargo la emisión de las leyes, muchas veces crean leyes injustas que favorecen a pequeños grupos en detrimento de la mayoría ciudadana.

2. ¿Qué es la desobediencia civil?

Derivado de las viejas reflexiones de John Locke, si un gobernante oprime a sus representados o actúa de manera contraria a los fines para los cuales fue designado, el pueblo tiene derecho a no acatar sus mandatos, pudiendo rebelarse con ánimos de destituirlo. Para los objetivos de esta investigación, usaré como definición de referencia, entre las muchas que teóricos y pensadores han expuesto, una de las más ampliamente aceptadas de desobediencia civil y que Hugo Adam Bedau expone en su *On Civil Disobedience*.¹³⁹ «Alguien comete un acto de desobediencia civil, si y sólo si, sus actos son ilegales, públicos, no violentos, conscientes, realizados con la intención de frustrar leyes —al menos una—, programas o decisiones de gobiernos.»

¹³⁹ Publicado en *Journal of Philosophy*, No. LVIII, Estados Unidos, 1963, Pág. 661.

Uno de los deberes fundamentales de una persona que vive dentro de un marco jurídico es obedecer las leyes; por tanto, desobedecerlas implica no encajar, no estar de acuerdo o considerarlas injustas. Entonces, surge la pregunta, respecto a nuestra investigación, ¿por qué los ciudadanos guatemaltecos podrían acudir a la desobediencia civil, que es una forma de resistencia? En primer lugar, porque está garantizada en la *Constitución*, en el artículo 5º: «Toda persona tiene derecho a hacer lo que la ley no prohíbe; no está obligada a acatar órdenes que no estén basadas en ley y emitidas conforme a ella.», además, en el artículo 45 de la misma *Constitución*: «Es legítima la resistencia del pueblo para la protección y defensa de los derechos y garantías consignados en la Constitución.» En segundo lugar porque, para el normal desarrollo de las relaciones sociales entre los ciudadanos, es fundamental que estos tengan confianza en sus autoridades; al no tenerla en la eficacia del Estado, a través de sus gobernantes, para el cumplimiento de las leyes, el pueblo tiene el legítimo derecho de exigir que las autoridades la cumplan para fortalecer el Estado de Derecho y, también, porque son las autoridades quienes deben constituirse en un ejemplo para la ciudadanía. Como colofón, queda la reflexión de Rousseau, en *El Contrato Social*, en el capítulo XVIII, del Libro III: «Doy aquí por sentado lo que creo haber demostrado, a saber: que no existe en el Estado ninguna ley fundamental que no pueda revocarse, incluso el mismo pacto social, pues si todos los ciudadanos se reuniesen para romperlo de común acuerdo, es indudable que el acto sería legítimo.»

Antes de pasar a caracterizar la desobediencia civil, es preciso hacer un deslinde entre esta y la resistencia del pueblo, o legítima resistencia. La desobediencia, puede ser un acto personal que implica la conciencia de desobedecer la ley por considerarla ilegítima. La resistencia popular implica un acto colectivo en el cual el pueblo muestra su disconformidad con determinadas leyes o funcionarios en el ejercicio de sus funciones. Por ejemplo, ambas características tuvo la resistencia social que se dio en Guatemala durante 19 semanas en 2015: resistencia contra los mandatarios, que finalmente hizo que renunciaran el Presidente de la República y la Vicepresidenta de la República; por otro lado, resistencia para provocar las reformas a la *Ley Electoral y de Partidos Políticos*.

3. Características de la desobediencia civil

La desobediencia civil no es una acción que se ejerce de manera caprichosa; generalmente está fundada en razonamientos morales, éticos o políticos que cuestionan el proceder legal de las autoridades y le contraponen el proceder legítimo. Las principales condiciones de la desobediencia civil, según Emilio Alvarado Pérez, son las siguientes:

»1) En general, es ejercida por personas conscientes y comprometidas con la sociedad —es lo que Hannah Arendt denomina minorías cualitativamente importantes—, lo cual les lleva a ser tan activas como críticas respecto a ciertas decisiones políticas que se han transformado en ley. La actividad desplegada por aquellos que ejercen la desobediencia civil es tan intensa y de tal naturaleza que

desborda los cauces tradicionales de formación y ejecución de la voluntad política. Los ciudadanos que practican la desobediencia civil son capaces de imaginar un orden social mejor y en su construcción la desobediencia civil se convierte en un procedimiento útil y necesario.

»2) Se entiende que el comportamiento de estos ciudadanos no está movido por el egoísmo sino por el deseo de universalizar propuestas que objetivamente mejorarán la vida en sociedad. Esta condición no niega que en ocasiones puedan coincidir intereses personales o corporativos con intereses de carácter general. Simplemente, pone de manifiesto que sería imposible consolidar un movimiento de desobediencia civil que únicamente se limitase a defender conveniencias particulares.

»3) Consecuentemente, los ciudadanos que la practican se sienten orgullosos. Para ellos, la desobediencia civil es un deber cívico más, es una exigencia que procede de ciertas convicciones a las que es posible atribuir un valor objetivo y constructivo.

»4) Por ello, es fácil adivinar que el ejercicio de la desobediencia civil ha de ser público, a lo cual contribuye también la pretensión de quienes la practican de convencer al resto de los ciudadanos de la justicia de sus demandas.

»5) Su ejercicio no vulnerará aquellos derechos que pertenecen al mismo bloque legal o sobre los que se sostiene aquello que se demanda. En cambio, su práctica podrá negar derechos de genealogía no democrática o que pretendan perpetuar privilegios injustificables. Entre las muchas consecuencias que se deducen de esta propiedad se encuentra la de que la desobediencia civil se

ejercerá siempre de manera pacífica. Por ello, la desobediencia civil se encuentra en las antípodas de las prácticas ligadas a aquellas filosofías irracionales que ven en la violencia la manifestación más pura de lo vital.

»6) Con ella no se pretende transformar enteramente el orden político ni socavar sus cimientos, sino promover la modificación de aquellos aspectos de la legislación que entorpecen el desarrollo de grupos sociales marginados o lesionados o, en su caso, de toda la sociedad.»¹⁴⁰

4. De la desobediencia civil al activismo político en la Internet

La desobediencia a las leyes es una realidad histórica y política que se ha desarrollado teóricamente, a partir de 1689 por John Locke. Este autor formuló que «cualquier ciudadano que sea oprimido por los gobernantes de un Estado tiene derecho a desobedecer sus mandatos e incluso a rebelarse contra ellos y destituirles.»¹⁴¹ La razón de lo anterior consiste en que «los gobernantes que “actúan contrariamente al fin para el que fueron instituidos [...] destruyen la autoridad que el pueblo les dio”»¹⁴²

Según Luis Gómez Romero en su ensayo *Desobediencia civil*,¹⁴³ citando a varios autores, se distinguen los elementos fundamentales de un acto de

¹⁴⁰ Emilio Alvarado Pérez, en: Reyes, Román, *Diccionario Crítico de Ciencias Sociales*, Editorial Plaza y Valdez, España-México, 2009.

¹⁴¹ Citado en: Gómez Romero, Luis, *Eunomia, Revista en cultura de la legalidad*, No. 6, España, Agosto de 2014, Pág. 239.

¹⁴² Gómez Romero, Luis, *Eunomia, Revista en cultura de la legalidad*, No. 6, España, Agosto de 2014, Pág. 239.

¹⁴³ Gómez Romero, Luis, *Eunomia, Revista en cultura de la legalidad*, No. 6, España, Agosto de 2014, Pág. 241.

desobediencia civil: «a) un acto que implica una violación a una norma de Derecho Positivo; b) una intencionalidad política manifiesta en dicha violación, que es concebida a modo de protesta pacífica en contra de la norma violentada; y c) el reconocimiento público por parte del agente del desacato de la antedicha norma, así como su aceptación de la correspondiente sanción.»

La desobediencia civil, como acción política, se manifiesta de distintas maneras, de acuerdo, primordialmente, al tipo de Estado que prevalezca en el momento de ejercerla. No es lo mismo practicarla bajo una dictadura que dentro de una democracia; en una monarquía que en una república; en estado de libertad, o en prisión.

La idea de desobediencia civil fue esbozada, en principio, en la doctrina liberal formulada por el inglés John Locke. Después, el estadounidense Henry David Thoreau la conceptualizó pero le dio a la desobediencia un carácter individual, que arranca a partir de tener conciencia sobre lo injusto de una norma o ley, como tomar la decisión de no pagar impuestos a un Estado que los recaudaba para fines que una persona considera injustos.

En 1848, Thoreau publicó el texto de una conferencia que denominó, precisamente, *Desobediencia civil*. En su escrito él manifestó su oposición a pagar impuestos a un gobierno que proclamaba la libertad pero que permitía la esclavitud y fomentaba la guerra injustificada contra México. Esas ideas las convirtió en acciones dos años antes de la publicación de su ensayo y, por ponerlas en práctica fue encarcelado. Su ensayo tuvo un éxito y resonancia enorme, a tal grado que fue utilizado posteriormente por desobedientes civiles tan

notables como Mohandas Gandhi, Martin Luther King, Nelson Mandela y otros líderes sociales de importancia.

Gandhi fue más allá de lo pensado por Thoreau; a partir de la opción individual, Gandhi la amplió hacia la opción colectiva. La desobediencia de Gandhi no tuvo solo motivaciones que partían de la conciencia personal sino que, también, implicaban la inconformidad colectiva ante la injusticia de una ley o ante la manera en que un Estado actuaba en contra de los ciudadanos. La estrategia que usó fue la no violencia activa, ya que consideró a la violencia como una manera inadecuada de resolver los problemas; por eso es famosa la frase que se le atribuye y en la que criticaba la famosa ley del talión: «Ojo por ojo y todo el mundo acabará ciego.» Para Gandhi la no violencia activa consistía en no quedarse de brazos cruzados ante una situación o ley injusta; por el contrario, en manifestar su repudio, inconformidad y rechazo a lo injusto a través de acciones no violentas. La lucha de Gandhi y la de Luther King les significó la muerte. Gandhi fue asesinado en 1948 y Martin Luther King en 1968. A partir de ellos se dio un paso enorme para que los pueblos volteasen sus miradas a los derechos inalienables del ser humano y a que la desobediencia civil fuese considerada como un acto por el cual, de manera no violenta, los ciudadanos pudiesen manifestar su inconformidad ante las leyes injustas y ante los procedimientos también injustos de un gobierno. Otro ejemplo a destacar respecto a la desobediencia civil fue el del líder sudafricano Nelson Mandela. Aunque su lucha comenzó de manera violenta, después comprendió que por esa vía no podría lograr sus objetivos.

En el ámbito latinoamericano también hubo destacados desobedientes civiles y luchadores que practicaron la no violencia activa. Uno de ellos, por mencionar el caso más cercano a Guatemala, fue Monseñor Oscar Romero. Él se opuso, a través de la palabra y la acción a que cesara la violencia en El Salvador. En ese contexto, el 23 de marzo de 1980, pronunció una larga homilía, que muchos juzgan como el detonante que apresuró su asesinato, ocurrido al día siguiente, 24 de marzo de 1980.

También se ha dado la vertiente armada de la desobediencia civil que no desembocó en enfrentamiento armado. Un caso ilustrativo para esta tesis es la del Ejército Zapatista de Liberación Nacional (EZLN), el cual surgió en 1994 como un movimiento armado e insurgente que retomó los ideales tradicionales de la izquierda marxista. Después, dio un golpe de timón hacia un movimiento étnico-reivindicativo, con un marcado cariz nacionalista. El proceso de resistencia y activismo político en Internet del EZLN mexicano, desde 1994 hasta el 2006, se fundamentó en llamar a la participación de la sociedad civil y de un proyecto político diverso y populista, que se dice en representación de los indígenas mexicanos, no solo chiapanecos, sino en representación también de la equidad de género. En 1994 denunció la grave problemática económica, social y política de marginalidad en que se encontraban las comunidades de Chiapas. El movimiento zapatista «hizo de la palabra su arma de lucha en la oposición al gobierno mexicano y de la acción colectiva su forma de resistencia». Las causas que

originaron el levantamiento del EZLN las divulgaron en la página Web zapatista: www.enlacezapatista.org.mx.¹⁴⁴

La legitimidad y legalidad del derecho a la resistencia civil está consignada en el artículo 45 de la *Constitución Política de la República de Guatemala*: «Es legítima la resistencia del pueblo para la protección y defensa de los derechos y garantías consignados en la Constitución.»

5. La información y los derechos humanos

La información pública se manejó en la realidad de épocas anteriores como información privada. Según las características estatales y gubernamentales, así también el trato que se le daba. Por ejemplo, en tiempos de Estrada Cabrera la información, como se ilustró en el capítulo II de esta investigación, se utilizaba fundamentalmente como fuente de conocimiento para determinar quiénes eran enemigos del gobernante y proceder a su represión o aniquilamiento; y así se siguió tratando hasta la época en que gobernó Jorge Ubico. Después, la información se utilizó para tipificar a los enemigos y amenazas contra la seguridad el Estado; tal tratamiento tuvo su culmen cuando se estableció el Estado contrainsurgente y cuyo fin ocurrió en 1996. En ninguno de esos momentos históricos se respetaron los derechos humanos. A partir de ese momento, empujado por las corrientes mundiales, varió el enfoque de la información pública

¹⁴⁴ Quintero Domínguez, Annie Erika. Resistencia y activismo político en Internet: el caso del Ejército Zapatista de Liberación Nacional de México (EZLN) 1994 – 2006. Universidad del Cauca. Facultad de Derecho, Ciencias Políticas y Sociales. Departamento de Ciencia Política, Popayán, 2010. Disponible en <http://consultoriasacademicas.com/wp-content/uploads/2014/09/tesis_annie_erika_quintero_resistencia_y_activismo_politico_en_internet.pdf>. Consultado el 20 de febrero de 2016.

que se centró en la seguridad ciudadana. Ese cambio, precisamente por el nuevo enfoque orientado hacia la ciudadanía, implicó de manera inevitable la inclusión de los derechos humanos, aunque en algunos aspectos todavía solo se dé en la teoría.

Los derechos humanos, en el ámbito mundial, comenzaron a tomar fuerza como práctica propiciada por los Estados, en buena medida a raíz de las reflexiones hechas por la humanidad respecto a los horrores experimentados en las guerras y en los Estados monárquicos y dictatoriales. En tal virtud, concluida la II Guerra Mundial, y después de un proceso que arrancó en el siglo XVII y tomó en cuenta pactos internacionales, declaraciones de los Estados, etc., la ONU recogió el espíritu que privó en todo ese proceso y elaboró, en 1948, la *Declaración Universal de Derechos Humanos*; en este documento, respecto a la información, como derecho humano, se establece, en el artículo 19, que «Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión.» Como se ve, el derecho a la información es tratado de manera escueta pero, posteriormente, se ha avanzado en su inclusión en las políticas públicas que los Estados han planteado ante la ciudadanía.

En un Estado democrático, como el que constitucionalmente se declara al Estado de Guatemala en el artículo 140 de la *Constitución*, existe la *Ley de Acceso a la Información* que tiene por objeto:

«1. Garantizar a toda persona interesada, sin discriminación alguna, el derecho a solicitar y a tener acceso a la información pública en posesión de las autoridades y sujetos obligados por la presente ley;

»2. Garantizar a toda persona individual el derecho a conocer y proteger los datos personales de lo que de ella conste en archivos estatales, así como de las actualizaciones de los mismos;

»3. Garantizar la transparencia de la administración pública y de los sujetos obligados y el derecho de toda persona a tener acceso libre a la información pública;

»4. Establecer como obligatorio el principio de máxima publicidad y transparencia en la administración pública y para los sujetos obligados en la presente ley;

»5. Establecer, a manera de excepción y de manera limitativa, los supuestos en que se restrinja el acceso a la información pública;

»6. Favorecer por el Estado la rendición de cuentas a los gobernados, de manera que puedan auditar el desempeño de la administración pública;

»7. Garantizar que toda persona tenga acceso a los actos de la administración pública.»¹⁴⁵

También, en el artículo 25 de la *Ley de la Comisión de los Derechos Humanos del Congreso de la República y del Procurador de los Derechos Humanos* se establece que «Toda persona, servidor o funcionario está obligado a

¹⁴⁵ Congreso de la República de Guatemala, Decreto No. 57-2008, Ley de Acceso a la Información Pública, Guatemala 2008, Artículo 1.

informar acerca de su gestión administrativa o comportamiento cuando se considere lesivo a los Derechos Humanos a requerimiento del Procurador, sus adjuntos o auxiliares departamentales. De no hacerlo así, el Procurador se valdrá de los preceptos constitucionales y legales para exigir tal información.»

En la Era de la Información en la cual vivimos y que comenzó en el último cuarto del siglo XX, y que en buena medida propició el avance tecnológico, sobre todo en el área de la informática, «No hay nada que no pueda ser cambiado por la acción social consciente e intencionada, provista de información y apoyada por la legitimidad. Si las personas están informadas, son activas y se comunican a lo largo del mundo; si la empresa asume su responsabilidad social; si los medios de comunicación se convierten en mensajeros, en lugar de ser el mensaje; si los actores políticos reaccionan contra el cinismo y restauran la fe en la democracia; si la cultura se reconstruye desde la experiencia; si la humanidad siente la solidaridad de la especie en todo el planeta; si afirmamos la solidaridad intergeneracional viviendo en armonía con la naturaleza; si emprendemos la exploración de nuestro yo interior, haciendo la paz con nosotros mismos. Si todo esto se hace posible por nuestra decisión compartida, informada y consciente, mientras aún hay tiempo, quizás entonces, por fin, seamos capaces de vivir y dejar vivir, de amar y ser amados.»¹⁴⁶

Sin embargo, estas «macro transformaciones» que trajo la era de la información, a la vez que han implicado enormes ventajas, también suponen muchos riesgos respecto al manejo indiscriminado de la información y sobre su

¹⁴⁶ Castells, Manuel, *La era de la información*, Siglo XXI Editores, México, 2009, Pág. 430.

empleo para fines que atentan contra los derechos humanos; por eso, una preocupación mundial para que el uso de la información no vulnere los derechos humanos ha dado como resultado que se hayan establecido normas para regular el derecho a informar y a ser informado, sobre todo en las redes sociales. Por ejemplo, en Youtube se restringe el uso de ese medio para mostrar videos considerados inadecuados, como pornografía. También se ha establecido, y es casi de uso general, que el usuario de la Internet tenga la posibilidad de aceptar o rechazar materiales que se le envían; de cancelar suscripciones, etc.

Por otra parte, «La **Asamblea General de la Organización de las Naciones Unidas** ha aceptado que el acceso a Internet es un derecho humano. A través de una declaración emitida por el relator **Frank La Rue**, el organismo internacional ha instado a los gobiernos de todo el planeta a que garanticen el acceso a sus ciudadanos.

»**Naciones Unidas** ha condenado a los países que filtren o bloqueen contenidos en Internet, ya que considera que, al permitir que los individuos ejerzan su derecho a opinar y expresarse —y en muchos casos, a disentir— es una herramienta que impulso el progreso social. “Asegurar el acceso universal del internet debe ser una prioridad de todos”, mencionó La Rue al dar a conocer esta declaración.»¹⁴⁷

El incremento del manejo de la información a través de soportes informáticos, ha incrementado de manera desmesurada la cantidad de información que una

¹⁴⁷ <http://hipertextual.com/2011/06/la-onu-declara-el-acceso-a-internet-como-derecho-humano>

Consultado el 13-11-2014, a las 10:03 horas.

persona puede manejar a través de esos soportes ya que evita la tardanza de la manualidad; tales ventajas también suponen desventajas y riesgos; en consecuencia ha dado lugar a que surja la tipificación del delito informático. «Este tema ha sido abordado por la legislación guatemalteca inapropiadamente, lo que provoca que muchas conductas delictivas queden fuera de sanción penal además estos delitos son investigados inadecuadamente, ya que por tratarse de una materia tan especializada, debiesen de existir procedimientos preestablecidos de recuperación y análisis de la evidencia que permitan la confiabilidad y validación de esta como medio de prueba.»¹⁴⁸

El delito informático puede definirse como «toda acción dolosa que provoca un perjuicio a personas o entidades en cuya comisión intervienen dispositivos habitualmente utilizados en las actividades informáticas.»¹⁴⁹

La información, a través de las redes informáticas, apenas si ha sido regulada en la legislación guatemalteca; por tal rezago, los riesgos que corre la persona emisora o receptora al manejar información son elevados; en consecuencia la vigilancia y provisión de seguridad a los sistemas informáticos suponen un costo adicional que siempre va en desmedro del usuario que por lo general es víctima de agresores poderosos, con mejor tecnología o con conocimiento más avanzados respecto a los sistemas informáticos. Por tal razón es de urgencia, aunque esto no resuelva todo el problema, que se propongan, discutan y aprueben leyes que protejan el entorno informático para aliviar, en

¹⁴⁸ Osorio Villagres, Herlindo de Jesús, Tesis *El peritaje de los delitos informáticos, aplicación y avances en Guatemala*, Universidad de San Carlos de Guatemala, Guatemala, 2012, Pág. i.

¹⁴⁹ Osorio Villagres, Herlindo de Jesús, *Op. Cit.* Pág. 1.

parte, el rezago que se padece en Guatemala respecto a este tema. Por otra parte, es preciso que las instituciones que manejan información pública y confidencial tengan especial cuidado, tanto en la selección del personal que manipula la información como en su formación, preparación e incentivo de conductas éticas. Un tema fundamental en este tema es el de legislar respecto a los agresores externos, como *hackers* y otros intrusos.

En la actualidad, la legislación guatemalteca tipifica el delito informático en el *Código Penal*, específicamente en el artículo 274 y sus incisos.

Pero más allá de legislar sobre los delitos informáticos y sobre el manejo informático, es preciso que la vigilancia del Estado sobre este aspecto esté fundado, sobre todo, en el respeto de los derechos humanos. Que a través del incentivo estatal se propicie una amplia discusión sobre este tema para que, de manera consensuada, la sociedad guatemalteca tenga la posibilidad de producir y recibir información con los menores riesgos de que sus derechos humanos sean vulnerados. Por eso, el avance tecnológico que se ha dado de manera acelerada, también propició en el plano mundial el nacimiento de una nueva generación de derechos humanos; es decir, la cuarta. Las diversas generaciones de derechos humanos son producto de su propia evolución; en ese sentido, los derechos previos a la cuarta generación son:

«**1. Los derechos de la primera generación** son los derechos civiles y políticos: los derechos que garantizan las libertades individuales (de expresión, asociación, religión, etc.) y la participación política (fundamentalmente, el derecho al voto). **Son los derechos a la libertad.**

«**2. Los derechos de la segunda generación** son los derechos económicos y sociales. Surgen como consecuencia de las revoluciones obreras de los siglos XIX y XX y de las distintas teorías socialistas. Así como los derechos de la primera generación consistían en la protección del individuo frente al poder del estado, estos derechos exigen una cierta intervención del estado para garantizar los bienes sociales básicos: educación, protección de la salud, trabajo, pensiones. **Son los derechos a la igualdad.**

«**3. Los derechos de la tercera generación** han comenzado a tener relieve a partir de la segunda mitad de este siglo. Son los derechos que tratan de proteger las libertades individuales frente a las distintas «poluciones» que las amenazan, como consecuencia de las nuevas tecnologías y de las perversiones del sistema económico. Estamos hablando del derecho a la intimidad, el derecho a disfrutar de un aire puro, el derecho a recibir una buena información, los derechos del consumidor, el derecho a la protección del patrimonio, el derecho, en general, a tener una vida de calidad. **Son los derechos de la solidaridad.**»¹⁵⁰

Los derechos humanos de cuarta generación todavía siguen en el plano de la discusión; no obstante, «Dentro de la gama de derechos de cuarta generación se pueden citar.»¹⁵¹

«• El derecho de acceso a la informática.

¹⁵⁰ Camps, Victoria, *Evolución y características de los derechos humanos. Los fundamentos de los derechos humanos desde la filosofía y el derecho*. Colectivo. EDAI, 1998, citado por Amnistía Internacional en: <http://www.amnistiacatalunya.org/edu/2/dh/dh-der-generaciones-camps.html>

¹⁵¹ CORDERO, Albert y CHAVEZ RODRIGUEZ. *Los Derechos fundamentales contenidos en el marco Jurídico que regula las telecomunicaciones del País después de la promulgación del Tratado de Libre Comercio con Estados Unidos y sus leyes complementarias*. Universidad de Costa Rica. Facultad de Derecho, citado en: <http://www.encuentrojuridico.com/2013/01/los-derechos-humanos-de-tercera-y.html>

«• El derecho a acceder al espacio que supone la nueva sociedad de la información en condiciones de igualdad y de no discriminación.

«• Al uso del espectro radioeléctrico y de la infraestructura para los servicios en línea sean satelitales o por vía de cable.

«• El derecho a formarse en las nuevas tecnologías.

• El derecho a la autodeterminación informativa.

• El derecho al Habeas Data y a la seguridad digital.»

En lo que respecta al ámbito guatemalteco, es fundamental que, dentro del Estado, se cree un sistema Nacional de Protección de la información.

6. Habeas Data y Protección legal de la Información

En dos artículos de la Constitución Política de la República de Guatemala se protege la información generada por cada persona, dentro del ámbito de la comunicación. La inviolabilidad es reconocida en el Artículo 24, el cual estipula: «Inviolabilidad de correspondencia, documentos y libros. Se garantiza el secreto de la correspondencia y de las comunicaciones telefónicas, radiofónicas, cablegráficas y otros productos de la tecnología moderna».

La importancia de la información estriba en la capacidad de identificar y que sea identificable. El titular de la misma es quien decide su destino final. Dentro del conjunto de datos que conforman la información, hay determinados aspectos de la vida que, si bien pueden mencionarse o se confían a cierta persona o entidad, no se pretende que el contenido de esa información llegue a un público masivo y desconocido, ya que estos «también describen aspectos más sensibles o

delicados sobre el individuo, como son los datos personales sensibles que tiene que ver con la forma de pensar, estado de salud, características físicas, ideología o vida sexual, entre otros.»¹⁵²

En el plano constitucional, únicamente se protege la información que pueda ser vulnerada en un ámbito de comunicación, pero no garantiza la protección de los datos que sean obtenidos por bases de datos privadas, las cuales utilizan esa información con propósitos mercantiles.

La *Constitución Política de la República* reconoce el *Habeas Data* en el Artículo 31. Pero esta garantía solo se refiere a archivos y registros estatales. Únicamente sobre esa información recae la autodeterminación informática del titular. Esta circunstancia es limitada frente a la amplitud que generalmente abarca el *Habeas Data* en otros países. Esta afirmación puede corroborarse con la reciente publicación (2015), de la Agencia Española de Protección de Datos.¹⁵³

En la Ley de Acceso a la Información Pública, Decreto Número 57-2008, se coadyuva en la transparencia informativa. El ciudadano puede verificar la información que acopian todas las entidades estatales. Este cuerpo normativo cumple con su finalidad, pero se requiere distinguir los propósitos de cada conjunto preceptivo, o bien, identificar su primacía en lo que se refiere al contenido

¹⁵² Cita extraída de la investigación sobre la Ley de Acceso a la Información Pública y Protección de Datos. Juárez, Rosa María, Hernández, Iris y Sánchez, Mario. Disponible en <http://www.redipd.org/actividades/talleres/La_Antigua_02_2014/common/Ponencias_Taller_La_Antigua./Guatemala.pdf>. Consultado el 20 de febrero de 2016.

¹⁵³ López Carballo, Daniel A. Protección de datos y habeas data: una visión desde Iberoamérica. XVIII Edición del Premio Protección de Datos Personales de Investigación de la Agencia Española de Protección de Datos. Disponible en: <https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/premios_2015/Proteccion_de_datos_y_habeas_data.pdf>. Consultado el 22 de febrero de 2016.

normativo. Con esta ley se pretende transparentar las actividades ligadas a la información en poder del Estado, pero no así la protección de los datos.

Los ciudadanos también cuentan con la autodeterminación informática sobre las bases de datos estatales, ya que pueden conocer, modificar o eliminar la información. Esto no se debe a la ley citada, sino por disposición del Artículo 24 de la *Constitución Política de la República*.

En relación con la protección de datos en Guatemala, no puede soslayarse la Ley de Derechos de Autor y Derechos Conexos, Decreto Número 33-1998. Esta normativa tiene la finalidad de proteger los programas de computadora y las bases de datos, por lo que también se relaciona con la protección informativa. Sin embargo, esta ley no contempla de manera amplia el significado del término datos, en lo que respectiva a la información de cada persona, sino que ingresa en el ámbito del Derecho Informático al referirse al «conjunto de bits que forman un programa o software».

Los programas de computadora y la producción sujeta a derechos de autor son los más violentados en las calles de Guatemala. Es normal encontrar copias ilegales por todas partes y esto nutre la economía informal, si bien la última ley citada busca enmarcar el ilícito de la reproducción indebidamente promovida.

También respecto a la protección de datos, en la Ley de Protección al Consumidor y Usuario, Decreto Número 006-2003, no hay disposiciones específicas, excepto el apercibimiento hacia los funcionarios de la entidad encargada de recibir las quejas por parte de los consumidores. La finalidad de

esta ley es proteger los datos del consumidor que realice una reclamación, siempre y cuando la queja se haya presentado por un medio electrónico.

En cuanto a la firma electrónica se cuenta con la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, Decreto Número 47-2008. En esta normativa se regula la validez de los datos, rigiéndose por el «principio de no repudio». Sitúa en condiciones de igualdad los datos obtenidos por un medio electrónico con los conseguidos por un medio tradicional como es el papel. Al abordar la Seguridad de la Información el enfoque es distinto en el comercio electrónico, la firma electrónica y las comunicaciones. Por un lado, los datos e información de los contratantes, legalmente, deben ser visibles y estar disponibles para su consulta, con la advertencia de que solo las partes contratantes y el tercero de confianza tienen la potestad de acceder a esa información.

La emisión de esta ley también obliga a emitir una normativa específica para prevenir, sancionar y erradicar los delitos de naturaleza informática que pudieran afectar el objeto o materia de la legislación sobre comercio electrónico, y también todos los actos ilícitos de naturaleza informática. Así se cumpliría con las pautas y reglas en el plano internacional, al tomar como base el Convenio sobre la Ciberdelincuencia suscrito en Budapest el 23 de noviembre de 2001. Este instrumento ha sido el modelo para regular la cibercriminalidad.

Hoy en día, Guatemala no cuenta con legislación especial que regule y sancione los delitos informáticos cometidos a través de sistemas que utilicen tecnologías de la información. Solo se encuentran algunas normas que fueron

adicionadas al Código Penal, Decreto 17-1973, las cuales no responden a las necesidades actuales, debido a la incontenible evolución de las tecnologías de la información.

Conclusiones

De acuerdo con lo investigado y expuesto en este trabajo, he llegado a las siguientes conclusiones:

1. Es viable unificar el sistema de denuncias del Sistema Nacional de Seguridad ya que esto es viable desde distintos ámbitos: humano, técnico y financiero. Existe capacidad humana para, en primer lugar, desarrollar el sistema de denuncias, y, luego, para desarrollarlo, ampliarlo y mantenerlo actualizado. Técnicamente es posible encontrar en el mercado, como ya se expuso en el capítulo III, el soporte digital y electrónico necesario; es posible que programadores puedan crear Bases de Datos electrónicas o adecuar los ya existentes para que la información, en especial sobre las denuncias, satisfaga las necesidades de la Inteligencia estratégica del Sistema Nacional de Seguridad. En lo que a financiamiento del equipo se requiere, como se evidenció también en el capítulo III, los costos no son desmesurados y pueden ser proveídos por el Estado o, incluso, ser proveídos por la cooperación internacional.

2. En la investigación se demostró lo eficaz que puede ser la unificación del sistema de denuncias en un solo conjunto, para que todas las instituciones del Sistema Nacional de Seguridad puedan aprovecharse de él y, a la vez, retroalimentarlo.

3. En el marco de las acciones programáticas que se desprenden de la Política Nacional de Seguridad, comprobé que debe institucionalizarse una base de datos

para el funcionamiento del sistema unificado de denuncias y se realice la Gestión del Conocimiento y la Gestión de la Información para cumplir las actividades de Inteligencia y Contrainteligencia, tanto del Sistema Nacional de Seguridad como del Sistema Nacional de Inteligencia.

4. La investigación evidenció que la integración de una base de datos no solo permitirá establecer la real dimensión del subreporte criminal en nuestro país, sino que además evaluará el impacto que tienen los programas de seguridad ciudadana, así como también la eficiencia y eficacia del sistema jurídico-policial. También permitirá constituir un modelo de prevención victimal, para atender de manera integral a las víctimas de la delincuencia y evitar que sufran de revictimización.

5. En el estudio es manifiesto que la aparición, desarrollo y masificación de las nuevas tecnologías de la información ha generado nuevas formas delictuales que tienen por medio o finalidad los sistemas informáticos y la Internet. Un efecto práctico de la arquitectura en red de la Internet es que los autores de los delitos cibernéticos no necesitan estar presentes en el lugar del delito. Por ello, impedir la existencia de refugios seguros para los delincuentes se ha convertido en un aspecto clave de la prevención de los delitos cibernéticos.

6. Hay indicadores de que la Internet se convirtió en el ámbito más democrático y participativo que las nuevas tecnologías de la información trajeron a un mundo que proclamó hace 67 años la Declaración Universal de los Derechos Humanos. En la actualidad, el espacio físico no será el único escenario bélico donde se diriman las

disputas de poder en todas las esferas, ni en donde se libren las guerras, en especial contra el tráfico de drogas y el crimen organizado.

7. Ante lo expuesto en esta investigación se llega a deducir que el derecho a tener acceso a la Internet debe ser considerado como un derecho humano, pues si bien no figura expresa expresamente en el inventario constitucional, al tenor del artículo 44 de la Constitución Política deviene inherente a la naturaleza humana el derecho a informar y ser informado, además de que este acceso es una facultad subjetiva, inalienable, imprescriptible, inembargable, de orden público, propulsor de la seguridad pública, la defensa nacional, la salud y la infancia, entre otros, pues su influencia penetra en todos estos aspectos.

Bibliografía

AECI, *Banco de información de los sistemas de seguridad social iberoamericanos*,

AECI, OISS Madrid, España, 1996.

Aguilera Peralta, Gabriel Edgardo, *Buscando la seguridad: seguridad ciudadana y*

consolidación democrática en Guatemala, FLACSO, Guatemala, Guatemala,

1996.

Altmark, Daniel R., *Informática y Derecho*, Depalma, Buenos Aires, Argentina,

1988-1991.

Altmark, Daniel R., *Informática y derecho: aportes de doctrina*

internacional, Depalma, Buenos Aires, Argentina, 1988-1991.

Alvarado Aguilar, Mabel, *Administración de la información EUNED*, San José, C.R.

2000.

Alvarado Porres, Julio Raúl, *La Informática en el ámbito legal*, Universidad

Francisco Marroquín Tesis, Guatemala, 1987.

Avila Valdés, Hugo Rolando, *Reducción de costos mediante el cálculo de la vida*

residual en equipos a través de la implementación de base de datos y la

administración del mantenimiento preventivo, USAC Tesis, Guatemala, 1998.

Azpilcueta, Hermilio Tomás, *Derecho informático*, Abeledo-Perrot, Buenos Aires,

Argentina, 1987.

Barahona Streber, Oscar, *Bases de la seguridad social en Guatemala*.

[s.l.] : Centro Editorial, 1946.

Becker, Hal B., *Análisis funcional de redes de información: enfoque estructurado*

del medio de comunicación de datos, Limusa, México, 1977.

Cancinos Franco, Raúl Arturo, *Administración de proyectos de un centro de cómputo*, Universidad Francisco Marroquín tesis, Guatemala, 1995.

Cano Betancourt, Francisco Rafael, *Acceso a la información sobre asuntos militares y diplomáticos de seguridad nacional: estudio de antecedentes de ley*, Universidad de Texas en Austin/Agencia Internacional para el Desarrollo Guatemala, Congreso de la República de Guatemala. 1999.

CanoM. Jeimy J., *Inseguridad de la información: una visión estratégica*, Alfaomega Colombiana, S.A., Colombia 2013

Coll-Vinent, Roberto, *Bancos de datos: teoría de la teledocumentación*. ATE, Barcelona, España, 1980

Cook, Melissa A., *Building enterprise information architectures: reengineering information systems*, Prentice Hall, Upper Saddle River, NJ, Estados Unidos, 1996.

CSUCA, *Manual de denuncia*, Comisión para la Defensa de los Derechos Humanos en Centroamérica CSUCA, Costa Rica, 1997.

Duarte López, Andrea del Camino, *La Responsabilidad internacional del Estado de Guatemala por obstrucción o falta de investigación a cargo de la Policía Nacional Civil y del Ministerio Público*, Universidad Francisco Marroquín, Tesis, Guatemala, Guatemala, 2011.

Falcón, Enrique M., *¿Qué es la informática jurídica?: del abaco al derecho informático*, Abeledo-Perrot, Buenos Aires, Argentina c1992

Feldstein De Cárdenas, Sara, *Contratos internacionales: contratos celebrados por ordenador. Autonomía de la voluntad. Lex mercatoria*, Abeledo-Perrot, Buenos Aires, Argentina, 1995.

Fernández Ovalle, Nelson Guillermo, *Ley que prohíbe a la PNC, identificar públicamente con nombres propios a las bandas delincuenciales: anteproyecto de ley*, Universidad de Texas en Austin/Agencia Internacional para el Desarrollo (AID), Guatemala, Guatemala, 2000.

Godínez García, Evelyn Yolanda, *Administración de proyectos orientada a la implementación de sistemas de información*, Universidad Francisco Marroquín, Tesis, Guatemala, Guatemala, 2003.

Godoy, Verónica; González, Fernando; Ramírez, Luis; Rodríguez, Alejandro, *Atención policial a las víctimas de delitos: estado de situación en Comisarías de la Policía Nacional Civil*, Instituto de Estudios Comparados en Ciencias Penales de Guatemala, Guatemala, Guatemala, 2006.

González Alvarado, Carlos, *Sistemas de bases de datos*, Tecnológica de Costa Rica, Costa Rica T 2000.

Grajeda Bradna, Walter, *Automatización de oficinas*, Fisicc-Idea, Guatemala, Guatemala: 1996

Henry, W. M, Leigh, J. A., Tedd, Lucy A., *Investigación con ordenadores búsqueda on-line*, ATE, Barcelona, España, 1980.

IEPADES, *Manual para el análisis y monitoreo de los presupuestos de seguridad y defensa*, Instituto de Enseñanza para el Desarrollo Sostenible, IEPADES / IDCR / CRDI, Guatemala, 2004.

Katsh, M. Ethan, *Law in a Digital World [electronic resource]*, Oxford University Press, New York, Estados Unido, 1995.

Kent, Allen, *Information analysis and retrieval* Wiley-Becker-Hayes, New York, NY, Estados Unidos, 1971, c1962.

Khadem, Riaz, *Administración en una página: cómo utilizar la información para lograr sus metas*, Norma, Barcelona, España, c1988.

La Haya, *Derecho internacional y derechos humanos*: La Haya, San José, C.R. 1996.

Larios Ochaíta, Carlos, *Derecho internacional público*, Maya' Wuj, Guatemala, Guatemala, 2010

Lessig, Lawrence , *The Future of ideas: the fate of the commons in a connected world*, Random House, New York, NY, Estados Unidos, c2001.

Ministerio Publico de la República de Guatemala, *Manual del Fiscal*, Guatemala 2001.

Organización Iberoamericana de Seguridad Social, *Banco de información de los sistemas de seguridad social iberoamericanos*, edición año 1996, Madrid, España, OISS, 1996.

Organización Iberoamericana de Seguridad Social, *Banco de información de los sistemas de seguridad social iberoamericanos*, edición año 1998, Madrid, España, OISS, 1998.

Palacio, Lino Enrique, *Derecho procesal civil*, V. 2, Abeledo-Perrot, Buenos Aires, Argentina, 1990.

Pazos, Luis, *Los ricos del gobierno: la costumbre de la corrupción*, Temas de Hoy, c2012, México, D.F., México, 1947.

Real Academia Española, *Diccionario de la Lengua Española*, Espasa Calpe, S.A. México, 2001.

Reynolds, Dennis, *Automatización de bibliotecas: problemática y aplicaciones*, Ruipérez, Madrid, España 1989.

Rivera Clavería, Julio, *Policía Nacional Civil en Guatemala: propuesta de reforma al sector seguridad y justicia*, Universidad Galileo, Instituto de Estudios de Seguridad, Guatemala, 2008.

Rojas Amandi, Víctor Manuel Vicente, *El uso de internet en el Derecho*, Oxford University, México, D.F., México, c2000

Rölz Bennett, José, *El Problema de la seguridad en la estimativa jurídica*, Universidad Nacional, Facultad de Ciencias Jurídicas y Sociales, Guatemala, c1941.

Saenz de Tejada Herrera, Guillermo, *Algunas consideraciones sobre los delitos de omisión USAC tesis*, Guatemala, 1948.

Seara Vázquez, Modesto, *Derecho internacional público*, Porrúa, México, D.F., México 2005.

Sierra González de Stalling, Marta Josefina, *El delito de omisión de denuncia como una deficiencia dentro del proceso penal guatemalteco*, USAC, tesis, Guatemala, 1995.

Scott, George M., *Principios de sistemas de información*, McGraw-Hill, México, 1988.

Stellino, Ana Isabel, *Política y seguridad nacional*, Gernika, México, México, 1996.

Tedd, Lucy A. *Introducción a los sistemas automatizados de bibliotecas*, Díaz de Santos, Madrid, España, 1988, c1984.

Thompson, Arthur A. Jr, *Administración Estratégica*, Mc Graw Hill, México 1999

Villalta Ramírez, Ludwin Guillermo, *El Ministerio Público de Guatemala: (un estudio: histórico, comparativo, descriptivo y propositivo)*, LM, Guatemala, 2008.

Vélez Mariconde, Alfredo, *Derecho procesal penal*, tomo I, Marcos Lerner Editora Córdoba, Córdoba, Argentina, c1981.

Zepeda Lecuona, Guillermo, *Crimen sin castigo: Procuración de Justicia Penal y Ministerio Público en México*, Centro de Investigación para el Desarrollo, A.C./Fondo de Cultura Económica, México, c2004.

VII.1 Material interactivo / apoyo informático (con reserva de que se utilizaron otros adicionales).

1. <http://www.juridicas.unam.mx>
2. <http://www.oas.org>
3. <http://www.la-alianza.org/index.php/denuncias>

