DEDICATORIA

A mis padres:

Luis Alberto Kouri Hanna (+)

Jenny Bumachar Farah

1° Edición 1,000 ejemplares
Lima - Perú, Julio 2016

Diseño de la cubierta y diagramación: Kinkos Impresores S.A.C
Hecho el depósito legal en la Biblioteca Nacional del Perú N° 2016-07809
Impreso por Kinkos Impresores S.A.C.
Av. Venezuela 2344 - Lima, Perú.

Índice

Introducción

En la actualidad, en la mayoría de penales del Perú (sobre todo los de máxima seguridad), existen de forma activa organizaciones criminales que suponen un peligro para la sociedad y el Estado. Por ello, la reflexión que se desarrollará plantea una alternativa para combatir la delincuencia que ocurre en el interior de dichos establecimientos. En la mayoría de estos lugares, se utiliza el bloqueo de celulares para evitar el crimen organizado; sin embargo no es la solución más adecuada, puesto que presenta limitaciones. Por lo tanto, se debe hacer uso de las herramientas de inteligencia para recolectar, procesar y utilizar la información obtenida a través de la interceptación de líneas telefónicas. A partir de ello, las autoridades tendrán los medios adecuados para enfrentar el crimen organizado, terrorismo, narcotráfico y sicariato, con lo cual podrán reducir el índice de criminalidad actual. Los métodos ya utilizados en los penales han mostrado ser poco efectivos: Se requiere de la interceptación de información para que el Estado no sea atacado en una guerra asimétrica de cuarta generación (4WG) por organizaciones criminales, en muchos casos, más poderosa.

En el primer capítulo se abordará la importancia que tiene la elaboración de inteligencia para enfrentar a las organizaciones criminales. Utilizando el flujo de información que se puede

encontrar en los distintos penales, se podrá recopilar datos e información que serán procesados para crear inteligencia que, posteriormente, agentes especializados utilizarán para desarmar crímenes. Ello es fundamental dado que la delincuencia no queda tan sólo en el ámbito interior; por el contrario, se afecta asimismo el exterior dado que los reos pueden seguir cometiendo crímenes sin ser realmente detectados y procesados por ello.

Se tratará, además, el sistema del bloqueo de señales, que se realiza a través de inhibidores, ya que se esperó que fuera una solución efectiva para enfrentar al crimen organizado en los penales y, sin embargo, ha probado su ineficiencia. Por ello, se plantea la interceptación telefónica legal conforme al ordenamiento legal vigente en los centros penitenciaros dado que, mediante la recolección de información de la comunicación que tienen los reos ilegalmente, se podrá combatir los delitos que cometen constantemente.

En el segundo capítulo se desarrollará la realidad del sistema penitenciario en el Perú. Ello hace referencia al control y organización real que se tiene dentro de los penales peruanos dado que, si bien hay un intento de las autoridades por mantener estructuras de organización, los reos, en la práctica, no tienen límites reales en lo que refiere a sus actividades. En más de una ocasión se han visto casos en los que los delincuentes tienen

acceso a objetos ilegales. Además es frecuente el que dispongan de dispositivos electrónicos, con lo cual pueden seguir teniendo un contacto directo con el exterior lo que resulta en la realización de una mayor cantidad de crímenes, especialmente de extorsión y coordinación con sus cómplices de otros tipos penales.

Asimismo, se verá que la instalación de inhibidores de señales en los centros penitenciarios es un facilismo que presenta grandes limitaciones y resulta perjudicial para la sociedad. Ello se debe, principalmente, a que, por un lado, el flujo de información de igual modo se mantiene a través de familiares y abogados que tienen contacto directo con los reos. Por otro lado, el bloquear la señal resulta en que las personas que viven en zonas adyacentes tampoco puedan tener una señal y comunicarse sin problemas puesto que el perímetro que abarcan los inhibidores no se puede delimitar precisamente. Es por ello que se explicarán las medidas adoptadas al respecto en diversos países para mostrar que los bloqueos de señal en los penales no han sido efectivos y, en muchos casos, ha sido necesario retirar los mismos.

En el tercer capítulo, se planteará la predominancia del bien común sobre el interés personal, ya que en las sociedades es importante que se busque y prevalezca el bien de todos los individuos sobre el interés particular. Con ello en consideración, se desarrollará el marco jurídico para la interceptación

de comunicación en el Perú en conjunto a las leyes de comunicación peruanas. Se podrá mostrar la importancia que tiene la interceptación legal de comunicación en los penales para poder enfrentar a las organizaciones criminales, terrorismo, narcotráfico y sicariato. Del mismo modo, se verá que en España se hace uso de la inteligencia, obtenida por el procesamiento de información, que se utiliza efectivamente a través de la interceptación de comunicación legal.

Por lo tanto, se hace evidente que se requiere de una propuesta para el caso peruano, dentro de la ley, en donde se haga uso activo de la inteligencia, mediante la interceptación, dentro del marco legal de las comunicaciones en prisiones, para enfrentar la 4WG.

CAPÍTULO I

Elaboración de inteligencia estratégica como arma en la guerra asimétrica (4WG)

1.1. La inteligencia estratégica

La inteligencia preventiva y prospectiva es una de las principales herramientas para enfrentar las diferentes manifestaciones de entidades no estatales en la generación de la guerra asimétrica (4WG), que compromete la acción conjunta de la policía y las fuerzas armadas. La inteligencia estratégica es un bien intangible, utilizado fundamentalmente para anticipar y predecir situaciones y circunstancias futuras puesto que en una estrategia de 4WG, la policía nacional y las fuerzas armadas tienen acciones de orden interno. Por ello, es que al elaborar inteligencia, es posible enfrentar efectivamente los conflictos que se presenten al permitir que la toma de decisiones sea la más adecuada por contraste de las diversas opciones de acción. De este modo, la inteligencia se puede definir como un "producto obtenido tras aplicar a la información técnicas de análisis, de forma que resulte útil al decisor a la hora de tomas sus decisiones con el menor nivel de incertidumbre posible, siguiendo el ciclo de la inteligencia".[1] Dicho de otro modo, la inteligencia es aquella información que ha sido analizada para que tenga un grado óptimo de verdad, permite la predicción de acontecimientos futuros y está orientada hacia un fin determinado. La inteligencia, al tener una finalidad específica, es producida para poder enfrentar a un enemigo o adversario que es perjudicial para los intereses del Estado. En esta lucha contra nuevas entidades no gubernamentales las tareas preventivas, disuasivas y represivas no deben estar reducidas al ámbito

1 DÍAZ FERNÁNDEZ, Antonio M. (Dir.) *Diccionario LID. Inteligencia y seguridad*. Madrid, 2013, p. 162. En adelante: *Diccionario LID. Inteligencia y seguridad.*

policial en el cuidado del orden interno según el mandato constitucional, sino además, por su condición supranacional en múltiples casos de los cárteles de la droga, sicariato, terrorismo y crimen organizado, la participación activa de las FFAA en su nuevo rol y readiestramiento son fundamentales.

En la inteligencia estratégica:

> "se distinguen tres niveles de decisión: 1) el nivel estratégico militar, que desarrolla la maniobra decidida en el nivel político estratégico y define la campaña con sus esfuerzos; 2) el nivel operacional, que tiene asignado un esfuerzo y unos recursos con capacidad para producir unos efectos, con acciones normalmente conjuntas; 3) el nivel táctico de las operaciones, donde se desarrollan las batallas y se convierte lo planificado en hechos, con acciones normalmente específicas. Para cada nivel de decisión, existe una estructura y organización de inteligencia".[2]

Para que la inteligencia estratégica pueda reducir el crimen organizado, es necesario que pase por un proceso en el cual se pueda distinguir la información que es útil. Con esta inteligencia se deben enfrentar situaciones que pongan al Estado en peligro para reducir las amenazas y el impacto de las mismas. Es por ello que la inteligencia estratégica está dirigida a múltiples funciones como "la obtención y análisis de información, la alerta sobre situaciones exteriores de interés militar con riesgo potencial de crisis, la detección y el seguimiento de crisis emergentes y el planteamiento y la conducción de operaciones

2 *Ibíd*., p. 168.

tanto bélicas como de mantenimiento de la paz".[3] La estructura y recursos de la inteligencia militar varían de acuerdo a cada Estado con sus respectivas instituciones, aunque en la mayoría de los países se cuenta con un órgano de inteligencia ya que este es indispensable para la organización militar.[4]

1.1.1. La información como insumo de inteligencia

Al hablar de inteligencia estratégica, se está haciendo referencia al procesamiento de información, con lo cual se hace evidente que la información es la materia prima de la inteligencia. La información es, en realidad, un conjunto de datos que han sido analizados para posteriormente convertirse en inteligencia; se trata de un proceso donde los datos iniciales se transforman en información que finalmente desarrollará la inteligencia. Los datos pueden ser múltiples y diversos; sin embargo, por sí mismos no poseen un valor real ni un significado específico. Al ser procesados como información recién empiezan a mostrar su relevancia.[5] Cuando las personas empiezan a realizar conexiones entre los datos, comienzan a interpretar y asimilar su

3 GONZÁLEZ CUSSAC, José Luis (coord.). *Inteligencia.* Valencia, Tirant Lo Blanch, 2012, p. 52. En adelante: *Inteligencia.*

4 En la inteligencia militar se pueden distinguir tres niveles de inteligencia: táctica, operacional y estratégica. La inteligencia estratégica es la que se encuentra en el nivel superior, seguida por la operacional y, finalmente, la táctica. Cada una cumple un rol fundamental en el Estado y posee una finalidad distinta.

5 Como ya se ha establecido, la información es parte del proceso para la producción de inteligencia; sin embargo, la información para ser tal requiere de datos. Con ello es que la información "Es todo aquel dato específico sobre algún hecho, fenómeno, persona o cosa en general. Como dato, constituye el antecedente necesario para llegar al conocimiento y es obtenido a través de los sentidos directa o indirectamente. Es específico porque es puntual en cuanto fija y determina en forma precisa su contenido". Escuela de Inteligencia Nacional (ESIN). *Manual de inteligencia estratégica del SINA. Aspectos básicos y comunes a todos los campos. Tomo I.* ESIN. Lima, 1997, p. 11. En adelante: Manual de inteligencia estratégica del SINA.

contenido para poder generar información pertinente. Mientras se avanza en la producción de la inteligencia, la cantidad de datos e información disminuye, mientras que la calidad de estos aumenta considerablemente para que la inteligencia sea concisa y verdadera.[6]

El transformar los datos en información requiere que el receptor y generador de los datos tengan un código en común, además del conocimiento previo que posean los agentes. Debe posibilitarse el entendimiento entre ambos para que la información procesada sea legítima. La información tiene un significado según quien la haya producido y depende del receptor el poder comprenderla para poder producir conocimiento e inteligencia. Debido a que la información siempre tiene el potencial de producir conocimiento, es el receptor quien debe tener una posición objetiva para determinar si es que la información brindada y obtenida es válida, útil y pertinente.

Según el modo en el que la información sea utilizada y cumpla una finalidad, posee un doble valor: instrumental e intrínseco.

> "El valor intrínseco proviene del simple hecho de que existe, en cuanto recurso capaz de originar conocimiento en algún momento de su existencia, y depende de la calidad de su almacenamiento, su organización y su proceso

6 La actividad de inteligencia es el "Proceso de búsqueda, recolección, apreciación, difusión y protección de información relevante y oportuna para la toma de decisiones en materia de seguridad y el buen funcionamiento del Estado." Por ello es que la información es el insumo imprescindible para obtener la inteligencia. *Diccionario LID*, p. 27.

> de comunicación. En cambio, el valor instrumental de la información está relacionado con su adecuación a las necesidades y el perfil del usuario y a su aplicabilidad práctica e inmediata por parte de éste para realizar un propósito específico en un contexto determinado."[7]

A partir de ello es que se puede establecer el valor de la información y el modo en que puede ser determinante para la producción de conocimiento y, fundamentalmente, de inteligencia.[8] La información, por otra parte, siempre debe producirse de acuerdo al requerimiento de inteligencia y es necesario que sea adquirida por quien podrá utilizarla eficazmente. Cualquier información no posee valor alguno si es que, por un lado, no es el momento adecuado para su uso o si, por otro lado, la persona que la ha obtenido no está en capacidad de utilizarla.

> "En un contexto donde la cantidad de información disponible supera en mucho las posibilidades humanas de adquisición y absorción y en el que la calidad oscila fuertemente, es necesario utilizar métodos y técnicas apropiados para identificar, recolectar, tratar analizar y evaluar información relevante con vistas a favorecer su uso y su transformación en conocimiento y en inteligencia. La información que es útil a la organización es aquella que atiende a sus necesidades y requisitos, que está disponible en el momento oportuno y que se dirige a la persona adecuada".[9]

7 Inteligencia, p. 21.

8 La utilidad e importancia de la información depende en especial de las habilidades humanas de adquisición y decodificación dado que es importante que se produzca un análisis, recolección, identificación y evaluación de la información obtenida.

9 *Ibíd.*, p. 101.

Por lo tanto, se requiere de un sistema de gestión de información eficaz, que pueda procesar la información para que pueda ser útil. El sistema de gestión debe estar dispuesto a transformaciones según corresponda dado que mientras más información se obtenga, más variará el proceso y los resultados. Por otra parte, una característica de la información es que siempre debe ser objetiva ya que no debe estar determinada por lo que se espera obtener sino que, más bien, se requiere de precisión y veracidad para que pueda ser imparcial. En consecuencia, la información no puede analizarse según las interpretaciones personales o interesadas, sino que debe contrastarse en todo momento con la información obtenida. La información procesada puede estar relacionada tanto al pasado como al presente y al futuro; además no requiere de una especialización particular para su entendimiento aunque es un especialista o analista quien está en capacidad de generar inteligencia a partir de ella.

1.1.2. Elaboración de inteligencia

La producción de inteligencia no se limita tan solo a la recolección de información sino que, por el contrario, se trata de un elaborado proceso que permite obtener la inteligencia como un producto veraz. Los datos e información se someten a un ciclo en el cual se analiza, evalúa y contrasta todo el conocimiento adquirido. A partir del proceso en el cual se produce la inteligencia, también se desarrollan principios que caracterizan la obtención de la misma. Entre los principios que guían la labor de inteligencia se encuentran los siguientes: finalidad, unidad de dirección, continuidad, objetividad, integridad, seguridad, oportunidad y flexibilidad.

Según el Servicio de Inteligencia Nacional del Perú[10], cada uno de estos principios tiene un rol fundamental para que la elaboración de la inteligencia sea la correcta. En primer lugar, la finalidad como principio busca que el proceso de inteligencia esté orientado a resolver una determinada situación, siendo fundamental para que la inteligencia pueda ser elaborada según su utilidad. La unidad de dirección, en segundo lugar, refiere a que la elaboración de inteligencia debe ser realizada por un mismo organismo, para que la información pueda ser procesada adecuadamente sin omisiones o duplicidades; es decir, se requiere de una unidad de dirección y técnica que pueda llevar el proceso a un objetivo común. En tercer lugar, la continuidad permite que se elabore constantemente inteligencia, ya que la información es un insumo que se actualiza permanentemente. La objetividad, en cuarto lugar, se requiere durante toda la elaboración de inteligencia, ya que los hechos deben ser tratados según se presentan sin que se pongan por encima los intereses particulares; debido a que durante el proceso se ven involucrados múltiples individuos, es importante para que la inteligencia sea válida que no se produzcan falsas interpretaciones. La integridad, en quinto lugar, responde al ciclo de producción de inteligencia, siendo fundamental que se cumpla cada etapa para que el producto sea el adecuado. En sexto lugar, la seguridad logra que el enemigo o adversario no tenga acceso a la información sobre la actividad de inteligencia. En séptimo lugar, el principio de oportunidad se establece para que el producto llegue a quien la necesita en el momento

10 Cfr. *Manual de inteligencia estratégica del SINA*, pp. 24-27.

adecuado ya que de no ser así, todo el proceso de inteligencia y la inteligencia misma pierde valor. Por último se encuentra la flexibilidad la cual tiene en consideración que las situaciones y oportunidades varían continuamente durante la producción de inteligencia y es necesario que los individuos puedan adaptarse y adoptar los procedimientos más convenientes a partir de ello.

Por otra parte, las etapas y el proceso varían según diferentes autores, pero el resultado siempre es el mismo: inteligencia. Según LID,

> "Tradicionalmente se consideraban cinco etapas: dirección y planificación de la obtención de información, búsqueda de datos e información, procesamiento de los datos e información; análisis de la información y producción de inteligencia; y difusión de la información. En la actualidad, tiende a considerarse un ciclo de inteligencia de seis etapas, en el que se añade a las cinco mencionadas la retroalimentación (…)".[11]

A partir de la ESIN (Escuela de Inteligencia Nacional)[12] y González Cussac (2012)[13], se desarrollarán las principales etapas del ciclo de inteligencia. La primera etapa consiste en la planificación, orientación y dirección de la búsqueda de información. Se requiere de un plan de desarrollo en el cual los órganos directivos y ejecutivos del servicio de inteligencia son quienes evalúan las prioridades para la búsqueda y obtención

11 Diccionario LID. Inteligencia y seguridad, p. 164.
12 Cfr. *Manual de inteligencia estratégica del SINA*, pp. 30-31.
13 Cfr. *Inteligencia*, pp. 135-162.

de información. Es, en esta etapa, en la que se deben establecer los objetivos principales y específicos de inteligencia, para que todo el proceso pueda estar orientado hacia una determinada finalidad. Por lo tanto, es fundamental que se tenga en cuenta durante esta fase, tanto el alcance que se tiene para producir la inteligencia esperada, como el presupuesto, plazos y asignación de medios y recursos humanos y materiales. Es en la planificación en donde se debe evaluar la posibilidad de obtener información y los respectivos medios de adquisición. Debido a que el proceso de inteligencia es dinámico y cambiante, la planificación continúa durante las siguientes etapas.

La segunda etapa es la búsqueda u obtención de información. Es esta fase, en la que se explotan sistemática y ordenadamente las fuentes de información. Se trata de adquirir toda la información pertinente que corresponda a los objetivos ya establecidos durante la planificación. Para obtener la información adecuada, se utilizan todos los medios, procedimientos y recursos que se tengan a disposición para que, posteriormente, sea posible su procesamiento. Un problema común para la obtención de información es, por un lado, la dificultad y escasez para conseguir información sobre determinadas áreas y, por otro lado, el exceso de información en otras áreas de interés. También se debe tener en cuenta que la obtención de información se puede complicar ya que se trata de una mercancía cara y su adquisición tiene un precio que en algunas ocasiones no resulta conveniente.

La tercera etapa corresponde al procesamiento de información. Ello consiste en la validación, organización y control de la información según su clase, valor y especificidad, para poder incorporarla a una estructura de información existente en la cual sea posible el acceso y recuperación. En algunos casos, la etapa de procesamiento también abarca tareas de traducción, desencriptación, desciframiento y decodificación. Se suele utilizar en esta fase una inteligencia múltiple que consiste en no aceptar un único tipo de información, sino más bien incorporar, integrar y analizar información y datos que correspondan a fuentes diversas. [14] Ello, por otra parte, permite que la información no se vea sesgada o influenciada al provenir de una misma y única fuente; el uso de fuentes diferentes permite una mayor objetividad y, por ende, una inteligencia valiosa y veraz. Según se va procesando toda la información obtenida, se la clasifica de acuerdo a su relevancia y valor para la producción de inteligencia. Ello no implica que una fuente sea superior a la otra, sino que determinadas fuentes son más apropiadas para cumplir los objetivos planteados.

La cuarta etapa es la elaboración de inteligencia. En esta etapa ya se distingue claramente entre la información y la inteligencia dado que posteriormente a esta fase la inteligencia, está lista para ser difundida o comunicada. Esta fase es similar al procesamiento de información aunque en esta etapa ya se

14 En el pasado, la inteligencia se denominaba según el tipo de información que se procesaba para obtenerla: inteligencia de señales o inteligencia humana. Sin embargo, debido a los avances para la obtención de información y a la tecnología disponible, es posible utilizar múltiples fuentes de información para producir inteligencia.

precisa lo que se convertirá en inteligencia según la evaluación de analistas y especialistas. La información obtenida y procesada se transforma en inteligencia de acuerdo con los principios que debe cumplir la inteligencia para que sea válida. En general, la elaboración consiste en la ejecución de actividades como la evaluación de credibilidad, pertinencia y fiabilidad de la información adquirida; la integración de la nueva información con la ya existente y el análisis e interpretación realizado por especialistas. Durante la evaluación e integración se debe diferenciar entre la información inexacta, sin rigor y poco fiable, para que sea desechada y que la información precisa pueda ser analizada.[15]

La evaluación de la información pasa por diferentes personas capacitadas hasta llegar a los analistas, quienes serán los últimos en determinar si es que la información es adecuada para la elaboración de inteligencia, teniendo en cuenta las evaluaciones previas. Con la integración de información se podrá, además, contrastar lo obtenido para confirmar y analizar si es que hay correlación entre las fuentes y la información que ha proporcionado cada una de ellas. El análisis e interpretación de información suponen procesos complejos en los cuales los especialistas deben tener especial cuidado para que toda

15 El sistema para determinar la exactitud de la información varía según cada organismo. Una de las formas para precisar aquello es la siguiente: "Por ejemplo, la fiabilidad de una fuente se puede calificar con una de estas letras: A fiable, B en general fiable, C bastante fiable, D no siempre fiable, E poco segura, F fiabilidad no evaluable. Y la credibilidad del contenido se puede indicar con un número de esta escala: 1 confirmado, 2 probable, 3 posible, 4 dudoso, 5 improbable y 6 exactitud no evaluable." Por ello si se tuviera información marcada como B5 se entendería que si bien la fuente es en general fiable, la certidumbre sobre su contenido es improbable. *Ibíd.,* p. 146.

la inteligencia elaborada sea imparcial. De este modo, la interpretación y el análisis deben ser realizados de modo simultáneo, al ser procesos complementarios. Se hace uso de inferencias que permitan una mejor comprensión y explicación de la información evaluada, sin embargo, la labor se complica ya que la información suele ser incompleta o intencionalmente encubierta por lo que depende del analista determinar y diferenciar entre los datos ciertos y los inciertos.

La quinta etapa es la comunicación o difusión de información, donde la inteligencia se distribuye a todos los individuos que tienen autorización para su utilización. Si bien toda la elaboración de inteligencia es entregada posteriormente a la realización de las etapas previas, durante el proceso se van entregando informes y estimaciones según sea necesario. En esta fase es de gran importancia que el mensaje llegue a tiempo, que sea apropiado según los objetivos planteados, que el contenido sea comprensible y claro, que el formato corresponda al canal de comunicación que se utilizará, y finalmente que la difusión se realice por medios seguros, manteniendo su carácter de confidencialidad según corresponda.

La sexta etapa, por último, refiere a la evaluación del proceso y es una etapa que fue incorporada para que el proceso sea más efectivo y retroactivo. Es importante conocer qué es lo que se realizó adecuadamente y qué es lo que debe mejorar para que en el futuro las operaciones de inteligencia se perfeccionen.

1.2. Crimen organizado y guerra de cuarta generación

El crimen organizado (terrorismo, sicariato y narcotráfico) constituye una amenaza continua que el Estado debe enfrentar. El peligro que suponen ha aumentado durante las últimas décadas para convertirse en un actor no estatal que utiliza medios poco convencionales. De este modo, el crimen organizado se puede definir como la

> "actividad o conjunto de actividades ilegales desarrolladas por organizaciones criminales o grupos criminales organizados con la finalidad de obtener y acumular beneficios económicos. El crimen organizado aparece frecuentemente asociado a la comisión de ciertos delitos específicos caracterizados por su particular gravedad o por constituir ocupaciones habituales de organizaciones o grupos delictivos organizados, entre estos destacan la extorsión y el tráfico de drogas, armas, personas y de otros bienes o productos, frecuentemente obtenidos por medios ilegales, así como el uso de la violencia con propósitos intimidatorios, la creación de estructuras comerciales o paracomerciales con fines de blanqueo y las prácticas de corrupción e influencia política. También conocido como delincuencia organizada".[16]

Asimismo, las organizaciones criminales son consideradas como una amenaza real en referencia a la seguridad nacional, ya que tienen un impacto a corto plazo y a largo plazo en donde las estructuras de la sociedad sufren graves daños.[17] Es debido al crimen organizado que la corrupción en el sistema político

16 *Diccionario LID. Inteligencia y seguridad*, p. 95.

17 Cfr. DE LA CORTE IBÁÑEZ, Luis y BLANCO NAVARRO, José María, et. al. *Seguridad nacional, amenazas y respuestas.* Madrid, Lid Editorial Empresarial 2014, p. 135.

se incrementa, con lo que la democracia y la igualdad política se ven afectados. De este modo se hace relevante el definir la guerra de cuarta generación que se relaciona directamente al crimen organizado, terrorismo y narcotráfico. Se trataría entonces de un

> "Conflicto de naturaleza descentralizada (…) que carece de una línea divisoria clara entre «la guerra» y «la política», o «los militares» y «los civiles». Además, lo caracterizan cinco rasgos generales: la lucha tiene lugar en un contexto complejo de conflicto de baja intensidad; acontecen tácticas y técnicas de generaciones anteriores; se lucha a través de un espectro de redes políticas, sociales, económicas y militares; se lucha mundialmente a través de estas redes e implican una mezcla de actores nacionales, internacionales, transnacionales y subnacionales. Este tipo de guerra suele implicar a un grupo violento que tiene como objetivo implantar su propio gobierno o restablecer un gobierno antiguo (…). A menudo, este tipo de conflictos tiende a desembocar en Estados fallidos y guerras civiles de distintos tipos, ya sea por cuestiones étnicas o religiosas."[18]

Por ello, es que resulta complicado el enfrentar a un enemigo que usa fuerzas irregulares o poco convencionales. Sería conveniente que se haga uso de la elaboración de inteligencia para desestabilizar al adversario. Tal como los grupos criminales han modificado sus estrategias, es necesario que el Estado busque nuevos medios para que se resguarde la seguridad nacional.

18 *Diccionario LID. Inteligencia y seguridad*, p. 151.

> "El camino hacia un orden mundial puede ser largo e incierto (…). Es altamente improbable que todas las partes, en especial aquellas que provienen de distintas tradiciones culturales, lleguen independientemente a las mismas conclusiones sobre la naturaleza y los usos permisibles de sus nuevas capacidades intrusivas. Es esencial definir una percepción común de nuestra nueva condición. A falta de eso, las partes continuarán operando sobre la base de instituciones separadas, magnificando las perspectivas de un desenlace caótico".[19]

La guerra de cuarta generación comprende además a la guerra asimétrica, con lo cual se muestra que el crimen organizado, narcotráfico, terrorismo entre otros, ha adquirido más poder y mantiene un enfrentamiento con el Estado. La guerra asimétrica se trata de una lucha entre el Estado y un ente no gubernamental - ya sea interno o externo - donde hay asimetría en lo que refiere a las capacidades logísticas y la capacidad de respuesta del uno con otro. Se podría hablar incluso, en algunos casos excepcionales, de Estados fallidos que combaten organizaciones que son más poderosas debido a su estratégica organización.

La guerra asimétrica, según LID, implica un:

> "Conflicto en el que los oponentes tienen características y ventajas estratégicas tan distintas que su confrontación se convierte en una pugna para forzar a la otra parte a combatir según sus propios términos. La estrategia es que el oponente débil suele adoptar consiste en golpear la base política doméstica de su adversario tanto como sus fuerzas

19 KISSINGER, Henry. *Orden Mundial, Reflexiones sobre el carácter de las naciones y el curso de la historia*. Madrid, 2016, p. 346.

> militares avanzadas. Esta estrategia implica infligir daños a lo largo del tiempo, sin sufrir como respuesta represalias insoportables".[20]

Suele ocurrir que los grupos a los que se enfrenta el Estado ya no son naciones dispuestas a luchar, sino más bien pequeños grupos clandestinos que poseen una estructura flexible y ramificada por lo que, al no contar con los mismos recursos que el Estado, hacen uso de medios poco convencionales para enfrentarse a él. La situación se complica cuando el adversario es apoyado por individuos y organismos con poder político o económico, que abusan de su autoridad, para beneficiarse a través del crimen organizado.

Otra característica del oponente en una guerra asimétrica es que "el adversario asimétrico es, en numerosas ocasiones, difuso, no tiene perfiles nítidos, oculta sus elementos, actúa en la sombra, es muy difícil de ubicar en un espacio concreto de acción y domina las artes de la decepción y de la desinformación".[21] Es por ello que los criminales suponen una gran amenaza al no poder determinar claramente sus desventajas y los medios adecuados para combatirlos.

1.3. Contrabando y uso ilícito de tecnología en prisiones

Debido a los continuos avances tecnológicos en telecomunicaciones que se han ido realizando en los últimos años, se ha hecho posible que en las prisiones los reos tengan

20 *Diccionario LID. Inteligencia y seguridad.*, p. 150.
21 Cfr. *Inteligencia*, pp. 76.

acceso a medios de comunicación ilegal, por medio del contrabando de los mismos. El fácil acceso a la tecnología en prisiones ha supuesto un problema para el Estado, el cual se ha envuelto en una guerra asimétrica con poderosas organizaciones criminales que tienen la posibilidad de seguir cometiendo crímenes incluso estando dentro de prisiones de alta seguridad. Por lo tanto, se ha evidenciado la necesidad de que el Estado enfrente esta amenaza del modo más adecuado.

El problema que suscita el permanente contrabando de tecnología en las prisiones es que estos centros de reformación se convierten, por el contrario, en lugares de ideologización criminal. Los reos, al seguir interactuando con el exterior tienen la posibilidad de seguir cometiendo crímenes. Tal situación acontecía ya desde la época del terrorismo en el Perú, en donde las cárceles se convirtieron, debido a la influencia de Sendero Luminoso, en trincheras de combate desde las cuales reclutaban a más personas para "proseguir la guerra popular"[22]:

> "We should start by understanding that in this prison, the activity of the Party has enabled the building of a Shining Trench of Combat, where we fight politically and ideologically against imperialism, revisionism and reaction. In this way it also becomes a school for all the prisoners. The masses get close to and recognise the leadership and authority of the Party that strengthens them ideologically and politically - which arms them against this sinister plan of the reactionaries to annihilate them. The love of the masses and the Party is great, powerful, indestructible."[23]

22 Cfr. RÉNIQUE José Luis. *La voluntad encarcelada. Las 'luminosas trincheras de combate' de Sendero Luminoso del Perú.* Texas, 2003, p. 37.

23 "Shining a light in the Darkness of Peru's Prisons". Interview with Comrade Inez. *World To Win*, 1999, N° 25.

De este modo, se utilizaron las prisiones para seguir cometiendo crímenes y, al mismo tiempo, incentivar y reclutar a más reos para que hagan lo mismo. Para conseguir que más personas se unieran a su lucha, se hacía uso de distintos recursos. Se trataba de una coacción que les permitiera alcanzar sus fines independientemente de los medios que se utilizaran.

> Every woman prisoner who arrives at the prison is subjected to tortuous harassment in order to try to break her and have her join their ranks. They utilise any method they can to try to accomplish their goals. They have physically assaulted the compañeras. The harassment is constant. Generally the newly arrived women prisoners are put into cells with these individuals. Here they dedicate themselves to harassing them twenty-four hours a day. If they cannot convince them, they try to break them down psychologically. (…) They look for every opportunity to provoke them, including organising "searches" with the guards in order to steal and destroy their belongings."[24]

Si bien se han dado una serie de avances en los últimos años, la realidad de los centros penitenciarios es la misma. El crimen es incentivado por otros reos y las organizaciones delictivas mantienen su poder, incluso cuando sus miembros se encuentran en prisión.

> "(…) prisoners are using contraband cell phones to conduct criminal activity. Although some facilities are making progress, correctional officials must be vigilant and use all available means to stop the phones from making their way to inmates in the first place. Nevertheless, the record indicates that prison authorities are devoting increasing financial

24 *Idem*.

> resources and personnel time to ferreting out, confiscating, and eradicating contraband cell phones in their prisons."[25]

Si bien en algunos casos se está intentando reducir el contrabando de celulares en prisión, a través de la confiscación y detección de los mismos, es una situación que sigue sin poder enfrentarse efectivamente. La mayoría de alternativas demandan compleja tecnología y técnica, regulación legal, instalación operacional, costos, entre otros. Cada una presenta ventajas y desventajas, lo fundamental es determinar qué opción sería la más beneficiosa para que el Estado no se vea amenazado.

La solución que se ha utilizado en los últimos años (en parte debido a su creciente popularidad) es la del bloqueo de señales, aunque resulta más perjudicial en la mayoría de casos. Es por ello que una alternativa más eficiente sería la elaboración de inteligencia para enfrentar esta situación mediante la interceptación legal de comunicación en prisiones.

1.3.1. La interceptación legal de comunicación en prisiones

El bloqueo de señales que ha sido propuesto por múltiples países para inhibir la señal en los penales, es en realidad, un facilismo. El flujo de información se mantiene, pero por vías que no pueden ser interceptadas como: los abogados, familiares

25 The National Telecommunications and Information Administration (NTIA). *Contraband cell phones in prisons: Possible Wireless Technology Solutions*. 2010, p. 37. En Adelante: *Contraband cell phones in prisons: Possible Wireless Technology Solutions.*

y amigos. A partir de ello es que una de las herramientas fundamentales para enfrentar el crimen organizado, terrorismo y narcotráfico es la inteligencia, que como ciencia, busca la información elaborada y debido a que la información es la materia prima fundamental para ello, cortar la información, es decir, el flujo de información o la cadena de información serían absolutamente contraproducente.

Por el contrario, el interceptar legalmente la comunicación de los reos en las prisiones de máxima seguridad, sería una alternativa de gran eficacia para enfrentar la situación mencionada. Tal interceptación consiste en "capturar comunicaciones realizadas en un sistema con el objetivo de tratar o investigar los contenidos obtenidos".[26] Sería beneficioso que, a través de la información obtenida gracias a la interceptación de señales, se elabore inteligencia que permita al Estado reducir los índices de criminalidad.

Lo que buscan los reos al acceder a dispositivos electrónicos, como los celulares, es continuar realizando crímenes y estar al tanto de lo que sucede en las organizaciones criminales de las que son parte. El uso que le dan a estos dispositivos es diverso y debido a que el contrabando es continuo, el acceder a celulares resulta sencillo.

> "Even if traditional wireline-prison-telephone services were provided free of charge to inmates, some inmates

26 *Diccionario LID. Inteligencia y seguridad*, p. 170.

> would continue to seek cell phones because they are useful, convenient, widely available, relatively inexpensive, and not subject to the monitoring safeguards imposed on legitimate prison telephone service. As discussed, convicted criminals have used contraband cell phones to intimidate witnesses and occasionally harm them. They have also used the phones to plan escapes, or run ongoing illegal enterprises through organized crime and gangs. While some incidents have made headlines, the number of crimes perpetrated through the use of contraband phones is difficult to estimate. For security reasons, prison officials are often reluctant to publicly release details of breaches that occur".[27]

Los crímenes que se cometen desde las prisiones siguen ocurriendo. Por ello, el utilizar legalmente la información obtenida a través de la comunicación que mantienen ilegalmente los reos por celulares de contrabando sería fundamental. Este sistema se conoce en otros países como *'bugging'*, *'intercepting'* o *'tapping'*. De este modo, las autoridades podrían acceder a la información que se encuentra almacenada en los celulares que han sido interceptados. Ello incluye tanto las llamadas como los mensajes de texto. Todo sin que la otra persona, en este caso el reo, sea consciente de que su comunicación está siendo interceptada. El 'tapping' es efectivo ya que el adversario no lo puede detectar.

> "Mobile phone tapping is based on a special software to be installed into the phone. According to its promoters,

27 FITZGERALD, Erin. *Cell 'Block' Silence: Why Contraband Cellular Telephone Use in Prisons Warrants Federal Legislation to Allow Jamming Technology. Wisconsin, Law Review*. Wisconsin, 2010, p. 1280. En Adelante: *Cell 'Block' Silence: Why Contraband Cellular Telephone Use in Prisons Warrants Federal Legislation to Allow Jamming Technology.*

> the tapping device can be installed within a few minutes. The tapping itself then runs as a hidden application which makes it absolutely undetectable. The only way to open this software in the mobile phone is to enter a special code. After entering this code a secret menu opens which allows further settings. Once installed, the tapping device is completely remote-controlled by text message commands".[28]

La elaboración de inteligencia prospectiva resultaría una alternativa más efectiva que la del bloqueo de celulares en prisiones, puesto que, como ya se ha desarrollado, la inteligencia permite a las autoridades controlar eficazmente diversos conflictos, en este caso la criminalidad dentro de prisiones de alta seguridad.

28 PORADA, V. et. al. *Environmental safety. Security in 21st Century.* Actas de la Universidad Politécnica de Odessa, 2013, p. 171.

CAPÍTULO II

La realidad del sistema penitenciario y la colocación de inhibidores de señales

2.1. Sistema penitenciario en el Perú

El sistema penitenciario en el Perú está orientado a reeducar, rehabilitar y reincorporar a los reos en la sociedad luego de cumplir con su sentencia. Durante el cumplimiento de su pena, los encarcelados son privados de su libertad, por lo que es necesario que el sistema penitenciario garantice que los reos sean tratados de modo digno y humano independientemente del crimen cometido. Sin embargo, lo usual es que ello sea obviado y las condiciones bajo las que viven los criminales sean inferiores a las ideales. En la mayoría de casos, los penales y prisiones en el Perú sufren de una gran sobrepoblación, por lo que se complica el cumplimiento de las sentencias indicadas. Todas las condiciones de vida en el sistema penitenciario dependen de factores políticos y económicos que varían constantemente:

> "La posibilidad de garantizar condiciones de seguridad que faciliten la convivencia, y la ejecución de los programas de tratamiento para la reinserción de la población penal, dependen en gran medida de la disponibilidad y calidad de las instalaciones físicas con que se cuente y del equipamiento que permita el cumplimiento de cada una de las competencias que con ese propósito deban ejecutar los operadores del sistema".[29]

Además, es de gran importancia que tal sistema tenga en consideración las características de los reos tales como su edad, género, delito y la condición del condenado.

29 DEFENSORÍA DEL PUEBLO. *El sistema penitenciario: componente clave de la seguridad política criminal. Problemas, retos y perspectivas*. Lima, 2011, pp. 27, 28. En adelante: *El sistema penitenciario: componente clave de la seguridad política criminal.*

2.1.1. Realidad del sistema penitenciario

Para desarrollar la realidad actual del sistema penitenciario peruano, es fundamental procesar las estadísticas que sean pertinentes para abordar el tema. Según los datos del INPE[30] desde octubre del 2014 a octubre del 2015 aumentó la población del sistema penitenciario total pasando de 87,226 a 92,400 reos, con lo cual la sobrepoblación que se da en estos penales incrementó. El porcentaje de sobrepoblación es la siguiente: en Puno un 74%, en San Martín un 40%, en Cusco un 116%, en Chiclayo un 133%, en Lima un 133%, en Arequipa un 138%, en Huánuco un 183% y en Huancayo un 205%. De este modo se evidencia que la sobrepoblación de los establecimientos penales en algunos casos duplica su capacidad con creces. Por último, de la población penal total el 2.91% está conformado por mujeres sentenciadas, el 3% por mujeres procesadas, el 45.86% por hombres sentenciados y el 48.23% por hombres procesados.

Debido a la tensión que se encuentra en los penales, es común que se den casos de violencia dentro de los mismos; se requiere de un control de orden y seguridad constante para erradicar los delitos que ocurren dentro de las prisiones y que repercuten tanto internamente como externamente según las circunstancias. Por ello, el personal debe estar capacitado para enfrentar tales situaciones y, de este modo poder:

30 Cfr. INSTITUTO NACIONAL PENITENCIARIO (INPE). *Informe estadístico penitenciario*. Ministerio de Justicia y Derechos Humanos. Lima, 2015, p. 5

> "-Garantizar la vida, la integridad física y psicológica de los privados de libertad;
>
> - Mantener el orden y la disciplina dentro del establecimiento penitenciario;
>
> - Evitar el ingreso de objetos prohibidos que alteren el orden o puedan significar un riesgo para la integridad de los privados de libertad, y del personal;
>
> - Impedir la evasión de las personas recluidas;
>
> - Supervisar el buen estado y funcionamiento de la infraestructura penitenciaria".[31]

Todo lo mencionado es necesario para el adecuado funcionamiento del sistema penitenciario. A pesar de ello, no es sencillo mantener el orden y control dado que la seguridad establecida no es suficiente. Lo que ocurre es que

> "Las deficiencias de seguridad anotadas favorecen la posibilidad de evasiones, hechos que sin lugar a dudas atentan contra la seguridad ciudadana. Por otro lado, la seguridad interna se ve afectada asimismo por el escaso número de personal asignado a estas labores. La supervisión realizada permite afirmar que la autoridad penitenciaria no puede controlar de forma efectiva los hechos que acontecen al interior de cada penal. (…) La infraestructura de seguridad interna, esto es, las celdas de reclusión y las rejas de los ambientes, también se encuentran en malas condiciones, lo que dificulta aún más la labor del personal penitenciario."[32]

31 *El sistema penitenciario: componente clave de la seguridad política criminal*, p. 32.

32 *Ibid.*, p. 35.

Son varios los factores que influyen en el funcionamiento correcto del sistema penitenciario y si alguno de ellos falla, el control se encuentra en peligro. Asimismo, para evitar el contrabando y delitos que se producen dentro de los penales, las visitas y comunicación de los reos deben realizarse siguiendo protocolos establecidos. Esto lleva a que la seguridad penitenciaria tenga cierto control sobre las visitas y lo que las mismas ingresan a los penales para evitar que los reclusos tengan acceso a drogas, armas, celulares, alcohol, entre otros.

Para la revisión de las áreas de encarcelamiento se pueden usar medidas ordinarias o extraordinarias en donde se realiza una revisión de las celdas con determinadas autoridades, para comprobar si es que los reclusos han adquirido objetos a través del contrabando. La revisión ordinaria se puede realizar semanalmente y participa, usualmente, el director o subdirector del establecimiento, el jefe de seguridad y el personal de tratamiento. En la revisión extraordinaria, participan las autoridades ya mencionadas junto al Ministerio Público y, si es necesario, cuentan con el apoyo de la PNP.[33] En lo que respecta a la comunicación de los presos, se cuenta con procedimientos de control para cartas y comunicaciones, además de que los reos tienen acceso a teléfonos públicos dentro de los penales. Sin embargo, la organización es deficiente y, por ello mismo, en múltiples ocasiones los delincuentes tienen comunicación con el exterior para seguir cometiendo crímenes.

33 Cfr. *Ibíd.*, p. 38.

2.1.2. Prisiones de máxima seguridad

Entre las principales prisiones de máxima seguridad en el Perú cabe destacar principalmente las siguientes: E.P. Lurigancho, E.P. Challapalca, E.P. Ancón I (Piedras gordas), E.P. Callao, E.P. Yanamayo y E.P. Castro Castro (ver anexo 2). En estos establecimientos penitenciaros, especialmente, se ha encontrado una sobrepoblación alarmante que sigue creciendo con el paso de los años. Además, suele haber problemas de orden y control por lo que los reos de estos penales suponen un peligro tanto para los individuos internos como para los externos[34].

En lo que respecta al penal de Lurigancho, la situación es grave debida la gran población que se alberga y el escaso personal de seguridad y tratamiento. Debido a la sobrepoblación en este centro penitenciario, las enfermedades se vuelven más peligrosas al estar tantas personas expuestas a ellas[35]. Por otra parte, el poco control que se tiene de los reclusos lleva a que éstos tengan acceso a artículos ilegales o de contrabando como droga, alcohol y celulares. Ello lleva a que se trate de "una población en constante riesgo por la promiscuidad en que viven, los abusos sexuales, el consumo de drogas, etc."[36]

34 Ello ocurre incluso al encontrarse dentro de estos centros donde se supone que pasan por un proceso de reeducación y rehabilitación como miembros de la sociedad.

35 También se debe mencionar que es uno de los penales en los que se reciben más visitas por lo que los reclusos son una especie de "población puente" en lo referente a la transmisión de enfermedades a la comunidad.

36 Comisión Episcopal de Acción Social (CEAS). *Perú: Informe sobre la situación penitenciaria.* Lima, 2005, p. 12. En adelante: *Perú: Informe sobre la situación penitenciaria.*

Durante los últimos años se han encontrado múltiples registros que muestran la vida de los reos dentro de este penal. En el 2015 se mostraron en la prensa imágenes en donde se veía a los reclusos con cervezas, piscinas (ver anexo 3), celulares y televisores.[37] Siempre y cuando tengan dinero, pueden acceder a cuantas comodidades deseen bajo los ojos de las autoridades y seguridad. Se trata de todo un sistema de corrupción y contrabando en los cuales se tiene acceso a diversos artículos:

> "Las imágenes, de la piscina corresponden al pabellón 11 A. La lata de cerveza se vende a 15 soles, el vaso de pisco sour a 8 soles. Para poder tener el celular se paga entre 50 y 100 soles semanales. Incluso para poder comer la paila se debe pagar 15 soles."[38]

Con todo ello, se evidencia que no hay una real regulación en lo que respecta a las visitas y a las actividades de los reclusos, ya que los grupos internos han logrado tomar el control. Se puede concluir que "en este penal no existen mecanismos adecuados para ser rehabilitados. Por el contrario, egresan del penal con mayores "conocimientos" y "estrategias" para delinquir".[39]

En la prisión de Piedras Gordas, la situación es muy similar a la que se vive en el penal de Lurigancho puesto que en este centro los reos también tienen un fácil acceso a dispositivos electrónicos que cuentan con internet. Uno de esos casos fue la

37 Cfr. El Comercio. *Penal de Lurigancho: presos tienen piscinas y discotecas.* Julio, 2015. http://elcomercio.pe/lima/ciudad/penal-lurigancho-presos-tienen-piscinas-y-discotecas-noticia-1825414 (última visita: 21 de marzo, 2016).

38 *Ídem.*

39 *Perú: Informe sobre la situación penitenciaria*, p. 13

del criminal "Colorado" que se encuentra encarcelado en dicha prisión ya que, mientras se encontraba cumpliendo su sentencia publicó mensajes amenazadores, en su cuenta personal de Facebook. Si bien la autoridad del penal, Genaro Escamilo Gómez, negó que ello fuera probable dadas las constantes revisiones a las que someten a los reclusos, reconoció que "en las requisas realizadas se han encontrado entre dos y tres celulares por pabellón, aunque aseguró que no tienen ningún caso de llamadas extorsivas desde este penal."[40]

Así mismo, el INPE encontró celulares y droga en las instalaciones del penal Castro Castro a mediados del 2015. Se trató de una operación sorpresa que duró siete horas, en la que se incautaron 387 celulares, 39 chips, 6 memorias USB, puñales y droga.[41] Los reclusos intentaron esconder los objetos mencionados al lanzarlos a los techos del pabellón, de igual forma, se consiguió decomisar el material para proceder con la denuncia de los reos responsables. Si el control de las autoridades del penal fuera el correcto, los reclusos no tendrían acceso a artículos tecnológicos y droga, por lo que se muestra, una vez más, que hay una ausencia de control con respecto a los criminales que pueden seguir cometiendo delitos desde el interior de los penales, sin mayores consecuencias. Debido a ello es que los reos, una vez que se han reincorporado a la sociedad,

40 El Comercio. *Preso de la banda de 'Caracol' lanza amenazas vía Facebook.* Enero, 2016. http://elcomercio.pe/lima/ciudad/penal-lurigancho-presos-tienen-piscinas-y-discotecas-noticia-1825414 (última visita: 21 de marzo, 2016).

41 Cfr. El Comercio. *INPE incautó 387 celulares y droga en el penal Castro Castro.* Junio, 2015. http://elcomercio.pe/lima/ciudad/penal-lurigancho-presos-tienen-piscinas-y-discotecas-noticia-1825414 (última visita: 21 de Marzo, 2016)

siguen cometiendo delitos, ya que no han sido reeducados y rehabilitados correctamente para vivir en comunidad, lo cual es en realidad el objetivo de los centros penitenciarios.

2.2. El facilismo del bloqueo de señales

El bloqueo o inhibidor de señales es un sistema en el cual, a través de un dispositivo electrónico, se anulan las señales transmitidas por celulares. Este sistema se ha aplicado en diversos países con determinadas regulaciones, aunque lo más común es que se apliquen en los centros penitenciarios para reducir el crimen y el contrabando de dispositivos electrónicos. A pesar de ello, ya se ha mostrado que este bloqueo es un simple facilismo dado que produce más problemas y, de igual modo, se siguen cometiendo diversos delitos dentro y fuera de los penales. En varios países se esperaba que el bloqueo fuera la alternativa eficaz para enfrentar el contrabando de cualquier dispositivo electrónico, siendo el celular el más frecuente.

> "They contend that the use of contraband phones poses dire consequences for the nation's justice system in the form of increased risk to victims, witnesses, jurors, and judges. Officials also fear a rise in successful escapes, prison riots, and further illegal activity conducted by incarcerated persons. Contraband cellular phones may even pose a risk to national security."[42]

La posesión de teléfonos de contrabando, de este modo, supone un gran riesgo tanto para las víctimas, testigos y jueces como

42 *Cell 'Block' Silence: Why Contraband Cellular Telephone Use in Prisons Warrants Federal Legislation to Allow Jamming Technology.* pp. 1272, 1273.

para la seguridad nacional. Si bien es cierto que a través del bloqueo se puede interferir con las señales, se mostrará que el bloqueo supone una alternativa fácil que no soluciona realmente la perpetuación de delitos desde el interior de prisiones. El "*jamming*" o bloqueo de señal supone una gran controversia y no ha sido aceptado en todos los países para el control del sistema penitenciario al tratarse de un sistema que aún no es completamente efectivo. Quizá puede contribuir al descenso de delitos de extorsión, pero no de otros ilícitos penales.

2.2.1. Políticas internacionales

Las políticas internacionales con respecto al uso de inhibidores de señal varían de acuerdo al país, con determinadas especificaciones respecto a su uso o prohibición. Se desarrollarán las medidas establecidas de los siguientes países: Reino Unido, Australia, Estados Unidos, México, Brasil, Colombia, Panamá, Honduras, Guatemala, El Salvador, Perú y Uruguay.[43]

En Reino Unido está prohibida la instalación o el uso de estos equipos, siempre y cuando no se haya solicitado una licencia previamente. En caso de que se haga uso sin una licencia hay una pena privativa de libertad de máximo dos años. En lo que respecta a las prisiones, también se empezó con la aprobación para la instalación de inhibidores de señal:

43 Cfr. GSM Association (GSMA). *Common position proposal on signal inhibitors (jammers) in Latin America*. 2014, pp. 14-21.

> "The prisons rule 2012 (interference with wireless telegraphy) received Royal approval on December 19, 2012. A motion of legislative consent was agreed by the Scottish Parliament on November 8 of 2011 to extend the provision within the rules of Scotland. Provisions began in England and Wales on 21 October 2013."[44]

En Australia, desde 1999 se tiene establecido que es ilegal suministrar, poseer u operar cualquier inhibidor de señal conocido como "*jammer*". Ello se debe a que consideran que "these devices have the potential to cause significant interference to legitimate radio services including, but not limited to, mobile networks".[45] Asimismo, si un individuo posee, opera o suministra estos dispositivos puede ir a la cárcel por dos años como máximo; incluso es posible que una persona sea condenada hasta cinco años, si es que se prueba que la interferencia que causó llevó a que la seguridad de otros individuos estuviera en peligro.

En Estados Unidos está prohibida la venta, publicidad o uso de los bloqueadores de señal. Sin embargo, su uso sí está permitido para el uso del gobierno federal. Además, en el 2013 se elaboró una propuesta para el desarrollo de un software que permita un control de acceso a la señal en los centros penitenciarios para combatir el contrabando de dispositivos electrónicos. "Managed Access technologies use wireless based stations positioned in prison to capture and block transmissions to

44 *Ibid.* p. 14.
45 *Idem.*

or from unauthorized devices."[46] Con ello es que se podría capturar y bloquear la señal de los dispositivos que no están autorizados, como lo serían los de los reclusos.

En México se puede hacer uso de los inhibidores de señal mientras que las autoridades estatales y federales estén involucradas con la cancelación de cualquier señal de telecomunicación. También se establece que el bloqueo de la señal no puede llegar a más de veinte metros fuera del perímetro determinado (el de la prisión, por ejemplo). De este modo, los inhibidores son suministrados y contratados por las autoridades pertinentes además de establecer mecanismos para resolver su efecto en usuarios.

> "A fundamental and crucial aspect is to establish an agreement of potential improvement and coordination between the authorities of federal and state levels for the successful implementation and effective operation of the inhibitors, to ensure the provision of the contracted service".[47]

Para el uso de estos dispositivos en este país, lo más importante es la cooperación entre las autoridades para que la implementación y uso de los mismos sea el correcto.

46 *Idem.*
47 *Ibid.* p. 15.

En Brasil se tienen regulaciones para el uso de bloqueadores de señal, aunque también es necesario que se tenga apoyo policial para detectar los dispositivos cuando son usados ilegalmente, dado que una vez instalados son difíciles de detectar y que la interferencia causada puede ser confundida como interferencia radial o falla del sistema. Siempre y cuando se sigan con las regulaciones establecidas por la ley, se permite el uso se estos dispositivos en las prisiones.

> "One aspect of potential improvement is the degradation of service in the surrounding áreas where these facilities are located and therefore customer complaints. Also, existing legislation could be modified imposing an almost total restriction on the private use of these devices, increasing penalties for noncompliance and its excepted use in specific security cases (as in prisons) being its use controlled by the administration."[48]

En Colombia se permite el uso de inhibidores de señal dentro de las prisiones y penales. Un problema recurrente es que la implementación y uso de estos dispositivos afecta a las áreas externas y por ello varios individuos se encuentran afectados. En dicho país, "it has been identified through researches the jammers and/or signal inhibitors generate impairment to the client, and operators are impacted negatively on their image and service provision."[49] Su uso afecta a los usuarios que se encuentran alrededor de estos lugares y, por ello mismo, la imagen de los operadores ha tenido un impacto negativo.

48 *Ibid.* pp. 15, 16.

49 *Ibid.* p. 16.

En Panamá también se permite el uso de bloqueadores para las prisiones y la implementación y operación de los mismos es responsabilidad de las autoridades competentes. Al igual que en Colombia, quienes viven en zonas adyacentes a la prisión se ven afectados por los inhibidores ya que no se puede determinar con precisión el perímetro en el cual serán bloqueadas las señales.

En Honduras está prohibido que los operadores móviles proporcionen servicios en las áreas específicas donde se encuentran centros penitenciarios, por lo que se ordena que se desmantelen las antenas o que se implementen otras soluciones técnicas para que en estos lugares no haya acceso alguno a señales. Como es el caso de otros países, la implementación de estas regulaciones perjudica a los ciudadanos que se encuentran cerca a estos lugares, dado que tampoco consiguen acceso a señal alguna.

En Guatemala, hasta el 2013, no había regulaciones específicas sobre los inhibidores de señal aunque sí estaba normada la regulación de llamadas y uso de celulares dentro de las prisiones. Por ello se tiene prohibido el uso de cualquier tecnología que permita la comunicación de los reclusos, dado que mediante estos dispositivos se llevan a cabo robos, extorsiones, secuestros, amenazas, etc.

> "(…) despite the importance of the use of mobile terminal equipment in communications in Guatemala, it can not be

> ignored that those goods are used as a tool to commit crimes such as robberies, extortions, kidnappings, assassinations, threats, among others, which is why within its scope it regulates the prohibition of use and possession of mobile terminal devices and any type of technology that uses SIM card, Micro SIM or any other type of mobile communication in all detention centres, prisons and correctional facilities, for both minors and adults".[50]

Además, los reclusos en posesión de dispositivos electrónicos, individuos que intenten ingresar cualquier dispositivo electrónico o trabajadores que faciliten a los reclusos el acceso a dispositivos electrónicos, serán castigados con una pena de libertad de seis años como mínimo. A partir del 2014, los operadores tienen la obligación de implementar soluciones técnicas para que no se pueda tener acceso a la señal desde las prisiones. Antes de esta resolución, se instalaron inhibidores de señal en algunas prisiones de Guatemala, pero su uso no fue efectivo, ya que eran sencillos de manejar para los prisioneros y afectaban a áreas que se encontraban a una distancia significante de las prisiones.

En El Salvador se ha ordenado a las operadoras móviles que, en las áreas de los centros penitenciarios, la señal que llega sea reducida para que los dispositivos electrónicos no puedan funcionar correctamente dentro de las prisiones. Una vez más, los ciudadanos que viven alrededor de estas zonas se encuentran gravemente perjudicados, ya que, como los prisioneros, ellos tampoco tienen acceso a la señal.

50 *Ibid.* p. 17.

En Perú la situación es compleja dado que desde el 2014 se inició con la instalación de inhibidores de señal en al menos 33 penales. Sin embargo, existen varios casos en los que, como se mostró anteriormente, los reclusos siguen teniendo un fácil acceso a dispositivos electrónicos por lo que secuestros, extorsión, amenazas y delitos siguen ocurriendo dentro de las prisiones.

Por último, en Uruguay, a partir del año 2000, no está permitida la instalación u operación de dispositivos que funcionen como neutralizadores de teléfono. Ello se debe a que se considera como muy perjudicial la señal que emiten estos dispositivos al ser el rango muy amplio. A pesar de ello, se han encontrado múltiples interferencias de señal generadas por bloqueadores que han sido instalados por compañías o individuos para que no se puedan utilizar teléfonos dentro de sus facilidades. Debido a que la instalación y configuración no ha sido realizada correctamente, la interferencia que se genera con estos inhibidores afecta enormemente a las personas fuera del rango deseado.

2.2.2. Sistema y limitaciones

Durante la última década se ha dado una transformación en la seguridad adquirida por las prisiones para enfrentar a las diferentes organizaciones criminales. Un medio que en un inicio fue ilegal pero que, con el paso de los años, se ha vuelto más común es el del bloqueo de señales. Estos dispositivos son conocidos como *'jammers'* y la tecnología que utilizan ha sido denominada como *'jamming'*:

> "Jamming techniques utilize a wide-band RF transmitter to transmit noise at the frequencies which are to be jammed. This noise makes it hard for communications to occur at the frequencies and therefore would inhibit the use of contraband cell phones in the area of interest. Jammers can be thought of as analogous to somebody shouting loudly in close proximity. The shouting will drown out most of the normal conversations making it difficult to talk normally. When this occurs in an RF communication system, the link between the cell phone and the tower cannot be made and results in a denial of service to the user".[51]

El bloqueo de señal consiste en el inhibir la radiación de señales deliberadamente, con la intención de interferir con la comunicación que se produce a través de dispositivos electrónicos.

> "A cell phone works by communicating with its service network through a cell tower or base station. These cell towers divide an area of coverage into cells, which range in size from a few city blocks to hundreds of square miles. The base station links callers into the local public switched telephone network, another wireless network, or even the Internet. A jamming device transmits on the same radio frequencies as the cell phone, disrupting the communication link between the phone and the cell phone base station, essentially rendering the hand-held device unusable until such time as the jamming stops."[52]

51 California Council on Science and Technology (CCST). *The Efficacy of Managed Access Systems to Intercept Calls from Contraband Cell Phones in California Prisons*. Sacramento, 2012, p. 60. En adelante: *The Efficacy of Managed Access Systems to Intercept Calls from Contraband Cell Phones in California Prisons*.

52 *Contraband cell phones in prisons: Possible Wireless Technology Solutions*, p. 13.

A pesar de que los dispositivos cumplen eficientemente la función de bloquear señales[53], tienen diversas desventajas. Por ejemplo, el bloqueo de señal que se emite no se puede disponer según espacios exactos por lo que, en muchas ocasiones, zonas alrededor de estas prisiones también se ven afectadas por el bloqueo de señal. Los inhibidores de señales no bloquean solo las señales prohibidas o de celulares de contrabando, sino que cualquier dispositivo electrónico que se encuentre dentro del rango establecido. Entre las funciones que tienen estos dispositivos se encuentra el bloqueo o interferencia de lo siguiente: comunicación por llamadas telefónicas, mensajes de textos y mails; conexión a wi-fi, funcionamiento del GPS, localización del dispositivo.[54]

El problema radica en que el uso de estos dispositivos es imperfecto y quienes rodean las zonas en donde están instalados los inhibidores se perjudican al no poder hacer uso de la señal.

> "(…) it is a complicated and imperfect science. Blocking cell phone signals tends to be more difficult than jamming other radio signals because phones operate at multiple frequencies. Cellular phones are able to "spectrum hop" within a frequency to avoid interference. Also, jammers must operate at a high enough power to block cellular signals within a desired range, but not so high that the jamming signals "leak" outside a particular area

53 Lo que hacen los dispositivos es transmitir ruido en las frecuencias que se han bloqueado, el sonido que se transmite hace que la comunicación no pueda ser escuchada por lo que los celulares de contrabando en las prisiones no funcionarían correctamente.

54 Cfr. Enforcement Bureau. *GPS, Wi-Fi, and Cell Phone Jammers Frequently Asked Questions (FAQs)*. FCC, http://transition.fcc.gov/eb/jammerenforcement/jamfaq.pdf (última visita: 20 de Marzo, 2016), p. 3,

> and cause disruptions to commercial wireless service or public-safety communications."[55]

No es sencillo conseguir que estos dispositivos funcionen como se espera, por lo que en más de una ocasión su uso se complica. Además de ello, uno de los problemas que supone este sistema es que la detección de dispositivos electrónicos, como celulares, sólo es posible cuando éstos se encuentran prendidos, por lo que no es posible detectarlos una vez que han sido apagados con lo cual la incautación de los mismos se dificulta.

Por estos motivos es que durante años el uso de esta tecnología fue ilegal en diversos Estados y países. Sin embargo, por el incremento de contrabando de celulares en prisiones, se empezó a probar estos dispositivos para enfrentar la situación:

> "(…) as the concern about contraband cell phones in prisons expands, there is growing interest in seeking exception to this law to allow jamming within the prison evironment. With the growing national concern regarding use of contraban cell phones both as a localized risk and a national security risk, there is renewed interested in seeking prison specific approval for use of jamming technologies".[56]

En algunos países se tiene absolutamente prohibido el uso de estos inhibidores, mientras que en otros es legal el uso expreso de los mismos para los centros penitenciarios[57]. Esta

55 *Cell 'Block' Silence: Why Contraband Cellular Telephone Use in Prisons Warrants Federal Legislation to Allow Jamming Technology*, p. 1282.

56 *The Efficacy of Managed Access Systems to Intercept Calls from Contraband Cell Phones in California Prisons.*, pp. 14, 15.

57 Entre los países que hacen uso de bloqueadores de señal para enfrentar el contrabando de celulares y crimen organizado se encuentran los siguientes: Francia, India, Irán, Irlanda, México, Nueva Zelanda, Suecia, entre otros. Además, en muchos otros países ya se ha propuesto su uso y se ha empezado a probar su alcance.

tendencia mundial de implementar los inhibidores de señal tiene actualmente en el Perú importante aprobación y asidero por parte de las autoridades competentes.

Si bien el sistema muestra algunos beneficios como la facilidad de su utilización, el bajo costo de su mantenimiento y la interferencia de comunicación, las desventajas son mayores.[58] Que no se pueda determinar precisamente un perímetro para su uso lleva a dos problemas fundamentales: el que se le niegue servicio a personas que se encuentran fuera de las prisiones pero dentro del rango de frecuencias y el que dentro de la prisión se encuentren zonas en donde es posible utilizar dispositivos electrónicos y tener acceso a señal, estos serían "*jamming deadspots*".

Por otra parte, en las prisiones sería evidente para los reclusos su implementación, dado que se muestra que ya no hay señal en zonas donde antes sí podían comunicarse libremente. Finalmente, los inhibidores de señal no evitan la filtración de información y la comunicación que se da entre los reclusos y sus abogados y familiares por lo que de igual modo habría un flujo de información que no podría ser utilizado para la elaboración de inteligencia.

58 Cfr. *The Efficacy of Managed Access Systems to Intercept Calls from Contraband Cell Phones in California Prisons*. p. 60.

CAPÍTULO III

La interceptación telefónica legal como vía efectiva para enfrentar el crimen organizado

3.1. El bien común frente al interés individual

El bien común[59] refiere al bien de una comunidad o sociedad donde se busca lo mejor para todos los miembros de la misma. Por ello, es necesario desarrollar el rol del bien común frente a la libertad individual, en relación al Estado.[60]

Desde la antigüedad esta noción ha estado vinculada con el poder político:

> "Platón (…) diseñó el Estado ideal de su República teniendo en cuenta esta idea, desde la que pretendió inspirar el proyecto social que propuso. En la obra platónica la estructura sociopolítica encontró justificación en la máxima aspiración de realizar la idea del bien. (…) Aristóteles (…) concibió al Estado como la resultante de una necesidad natural, la de vivir en sociedad, y vio su finalidad en el logro del bien común, que definió como felicidad e identificó con la vida virtuosa que se logra con la actividad contemplativa."[61]

El bien común político, requiere del respeto y promoción, tanto de los gobernantes como de los ciudadanos, aunque son los gobernantes quienes tendrán una mayor responsabilidad dado

59 Para la Doctrina Social de la Iglesia, el bien común refiere al "conjunto de aquellas condiciones de la vida social que permiten, ya sea a la colectividad como así también a sus miembros, alcanzar la propia perfección más plena y rápidamente". Pontificio Consejo Justicia y Paz. *Compendio de Doctrina Social de la* Iglesia. Librería Editorial Vaticana. Ciudad del Vaticano, 2005, p. 164

60 "El bien común no es un bien único, sino que forma un entramado de bienes de diverso ámbito y nivel, unos orientados a otros. (…) Es el resultado de la acción autónoma de individuos libres dentro de unas estructuras sociales y políticas que lo hacen posible". Antonio Argandoña. *El bien común*. Barcelona, 2011, p. 5.

61 MARTÍNEZ GÓMEZ, J.A. *El poder, el bien común y los intereses individuales y sociales*. Contribuciones a las Ciencias Sociales, 2011. En adelante: *El poder, el bien común y los intereses individuales y sociales.*

que establecen las normas y leyes que permiten la concreción del bien común. Es así que las personas se ordenan u organizan hacia un fin común gracias a las leyes:

> "el legislador humano (…) participando de la *tarea reunificadora* que dispone todas las cosas hacia el bien común universal, pone leyes a los hombres que forman parte de la comunidad que gobierna, cuando imprime en sus mentes, con un mandato o indicación cualquiera, una regla en vista de la conformación de la comunidad que dirige".[62]

El bien común puede ser, además, entendido como aquello que restringe la libertad individual dado que hay un vínculo entre todos los ciudadanos hacia la disposición de un bien común general.

> "Puesto que la realización personal no se logra en solitario, sino en comunidad, es preciso que el hombre (…) se disponga también adecuadamente a la convivencia con los demás. Y *el hábito por el cual el hombre se dispone adecuadamente para la convivencia es la justicia* (…) por la justicia lo que se afina es la propia voluntad para que quiera el bien del prójimo."[63]

Con ello se supone que el bien de los otros es el bien propio, con lo que el bien común sería al mismo tiempo el bien personal.[64] Quien deberá determinar la mejor forma para que los ciudadanos se encaminen al bien común será el Estado.

---

62 POOLE, Diego. *Bien común y derechos humanos*. Persona y derecho: Revista de fundamentación de las Instituciones Jurídicas y de Derechos Humanos. 2008, N° 58, p. 114.

63 *Ibíd*., p. 122.

64 Debido a que se trata de una sociedad con una finalidad, siendo el bien común tal finalidad, éste no puede ser reducido a los bienes particulares de sus miembros dado que se pretende lograr el bien que incluya a todos los individuos de la comunidad.

De este modo, hasta la modernidad el Estado es quien debe proteger el bien común que busca la mejor realización de los individuos que forman parte de una comunidad. "Para lograrlo el Estado tiene el monopolio de la fuerza que es ejercida sin reparar en las particularidades individuales, de ahí su carácter abiertamente totalitario y absorbente".[65] Se entiende, por lo tanto, que mientras que el Estado defienda el bien común, estará garantizando el bienestar y felicidad de sus miembros.

Durante muchos años se ha visto que el debate entre la privacidad y prevención del delito ha llevado a que determinadas medidas tecnológicas no puedan ser implementadas, con lo cual se puede evidenciar que no se ha tenido en cuenta el bien común de la sociedad.

> "(…) el discurso de los defensores de la privacidad no sólo ha incurrido en ciertos excesos retóricos (…) como resultado de ese estado de opinión (i) se ha venido a retrasar durante años la puesta en práctica de ciertas intervenciones públicas necesarias mediante su impugnación ante la justicia (…); (ii) se ha bloqueado la introducción de otras políticas públicas igualmente necesarias que entrañaban limitaciones en la privacidad de las personas; (iii) se ha producido un efecto de enfriamiento (…) en ciertas políticas públicas por miedo a las consecuencias del examen riguroso de ciertos colectivos (…); y (iv) se ha conseguido evitar la implementación de nuevos aparatos e instrumentos tecnológicos que podrían haber puesto una mejora tanto en la privacidad como en la sanidad pública".[66]

65 *El poder, el bien común y los intereses individuales y sociales.*

66 AGUSTINA SANLLEHÍ, José R. *El debate actual entre privacidad y prevención del delito: una propuesta comunitarista.* InDret, revista para el análisis del derecho. Barcelona, 2010, p. 6.

Ello en relación a la interceptación telefónica de comunicación legal indica que se debe buscar un balance entre la protección del delincuente y la defensa de la comunidad dado que el bien común prima sobre el bien particular.

3.2. Marco jurídico peruano para la interceptación telefónica legal

El marco jurídico peruano no autoriza la interceptación telefónica, si no se cuenta con el permiso correspondiente del juez competente. Por lo tanto, el Decreto Legislativo 1182 que permite la localización y geolocalización de los teléfonos de las personas denunciadas por delitos no contempla la interceptación de llamadas telefónicas ni obliga a las empresas telefónicas a brindar información sobre los contenidos de las comunicaciones.[67]

Sin embargo, hay un margen de acción en el cual los agentes de la Dirección Nacional Antidrogas (Dirandro) de la Policía Nacional del Perú cuentan con autorización para interceptar las comunicaciones telefónicas de delincuentes a través de un sistema de autorización judicial. Es así que, mediante un equipo llamado "Constelación", el equipo especial de la Dirandro espía alrededor de 300 líneas telefónicas diariamente.

67 Cfr. Noticia geolocalización

Asimismo, el gobierno del presidente Humala en el año 2013 adquiere, en el marco del "Plan Pisco", equipos para inteligencia electrónica a la empresa israelí Verint Systems Ltda. Con capacidad para interceptar simultáneamente tres mil líneas telefónicas con el supuesto propósito de ser utilizado en la lucha contra la criminalidad y el narcotráfico. Dicha adquisición fue complementada con la capacitación de personal de inteligencia electrónica y analistas para realizar esa tarea.

Es de gran importancia el distinguir cuál es la información que debe ser interceptada legalmente dado que los presos tienen derecho a la privacidad e intimidad. Es por ello que en las escuchas de comunicación telefónica legal lo que se obtiene y procesa debe ser de interés público y para el bien común de la sociedad. A partir de ello se requiere "distinguir el interés público en la información de la mera curiosidad, de forma que, por ejemplo, no sea lícito difundir cualquier tipo de información relativa a la vida privada (…)"[68]. El Tribunal Constitucional peruano, por lo tanto, establece lo siguiente:

> "(…) en relación a la interceptación de las telecomunicaciones y su divulgación por los medios de comunicación, está prohibida la difusión de información que afecte la intimidad personal o familiar, o la vida privada del interceptado o terceras personas, salvo que ella sea de interés o relevancia pública, lo que debe ser determinado en cada caso por el propio medio de comunicación. En caso de exceso tanto

68 MARCIANI BURGOS, Betzabé. *Interceptaciones telefónicas ilícitas, vida privada e interés público. O las marchas y contramarchas del Tribunal Constitucional en relación con la libertad de expresión de los medios de comunicación*. Instituto de defensa Legal – Justicia Viva. Madrid, 2010, p. 6.

> el periodista, como los editores y/o los propietarios de los medios de comunicación, serán responsables por tales excesos, según lo determine la autoridad competente"[69]

Asimismo, una interceptación telefónica ilegal, es decir, que no esté autorizada por un juez, está penalmente sancionada por el artículo 162 del Código Penal peruano. De este modo se establece que si bien nuestro marco jurídico en el Decreto Legislativo N° 1182 permite la identificación, localización y geolocalización de equipos de comunicación en la lucha contra la delincuencia y el crimen organizado, no se han establecido medidas ni leyes que permitan un proceso rápido y adecuado para la interceptación y escuchas de comunicaciones de modo legal en relación a la delincuencia y el crimen organizado.

3.2.1. Leyes de comunicación en relación a la delincuencia

El artículo 2, literal 10 de la Constitución Política de 1993, regula el que todo ciudadano tenga derecho al secreto y a la inviolabilidad de sus comunicaciones y documentos privados. De ello se pueden desprender dos puntos importantes, primero la titularidad del derecho y segundo los alcances de protección. Respecto del primer punto, resalta el que la norma constitucional no realiza diferenciación de sujetos titulares de este derecho; incluso el artículo 2.4.g establece que la incomunicación solo

69 *Ibíd.*, p. 8.

puede ser con fines de esclarecimiento de un delito. Si bien la misma norma suprema señala que el ejercicio del derecho a la ciudadanía se suspende en casos de sentencias con pena privativa de libertad, se excluye de esta limitación a los internos procesados y se mantiene respecto de los condenados. Sin embargo, tal suspensión solo hace referencia a los derechos políticos que se encuentran vinculados en específico al ejercicio de la ciudadanía, puesto que si bien tanto los derechos civiles y políticos son derechos humanos de primera generación, los civiles son de manera específica los derechos fundamentales.

Con respecto a las leyes de comunicación en el Perú, se debe distinguir que el marco jurídico tiene en consideración la privacidad e intimidad de los ciudadanos por lo cual en el artículo 4 de la Ley N° 28737, se dispone que toda persona tiene el derecho a la inviolabilidad y al secreto de sus comunicaciones siendo el Ministerio de Transportes, Comunicaciones, Vivienda y Construcción quien se encarga de proteger tal derecho. A pesar de ello, la ley peruana establece que se pueden interceptar comunicaciones siempre y cuando se tenga una orden judicial que otorgue el permiso para las acciones correspondientes.

Se debe destacar, además, que en al artículo 87 de la Ley N° 28737, entre las denominadas infracciones se encuentra la interceptación o interferencia no autorizadas de los servicios de telecomunicaciones no destinados al uso libre del público general, tanto como la divulgación de la existencia o del contenido, o la publicación o cualquier otro uso de toda clase de información

que haya sido conseguida a través de la interceptación o interferencia de los servicios de telecomunicaciones no destinados al uso público en general.

Si bien la persona al ingresar a un establecimiento penitenciario asume una relación de sujeción especial con la Administración, que implica una restricción de derechos, propio del cumplimiento del régimen de tratamiento que se le ha asignado, ello per se no significa una pérdida absoluta de sus derechos fundamentales; así lo ha establecido el Tribunal Constitucional peruano en la Sentencia del Expediente N° 0726-2002-PHC/TC, caso Alejandro Rodríguez Medrano:

> "En efecto, tratándose de personas privadas legalmente de su libertad locomotora, una obligación de la que no pueden rehuir las autoridades penitenciarias es la de prestar las debidas garantías para que no se afecte o lesione la vida, la integridad física y los demás derechos constitucionales que no hayan sido restringidos. Ello supone que, dentro de márgenes sujetos al principio de razonabilidad, las autoridades penitenciarias no sólo puedan, sino que deban adoptar aquellas medidas estrictamente necesarias para preservar los derechos constitucionales de los internos, cada vez que existan elementos razonables que adviertan sobre el eventual peligro en el que éstas se puedan encontrar".

De acuerdo a estas premisas, los internos mantienen sus derechos fundamentales básicos, al punto de su restricción necesaria para el cumplimiento del tratamiento penitenciario, dentro de estos se ubica el *derecho a las comunicaciones* y en

específico las telecomunicaciones[70], puesto que en línea de la Corte Interamericana de Derechos Humanos, las conversaciones telefónicas es una forma de comunicación que calza en el ámbito de la vida privada protegida por la Convención Americana: "El artículo 11 protege las conversaciones realizadas a través de las líneas telefónicas instaladas en las residencias particulares o en las oficinas, sea su contenido relacionado con asuntos privados del interlocutor, sea con el negocio actividad profesional que desarrolla".

Es necesario precisar que el derecho a las comunicaciones es el género, mientras que la especie es la telecomunicación y se considera al interno como un ser humano al cual el sistema penitenciario busca reinsertar a la sociedad. En cumplimiento de lo manifestado, el artículo 37 del Código de Ejecución Penal, regula el derecho a la comunicación del interno: "El interno puede comunicarse periódicamente, en forma oral y escrita y en su propio idioma, con sus familiares, amigos, representantes diplomáticos y organismos e instituciones de asistencia penitenciaria (…). Las comunicaciones se realizan respetando la intimidad y privacidad del interno y sus interlocutores".

Este reconocimiento del derecho a la comunicación tiene una restricción concreta en el caso de las telecomunicaciones, puesto que si bien no la restringe en absoluto sí ha implementado un

70 Tal punto hace referencia a los teléfonos públicos instalados y regulados por las autoridades de los centros penitenciarios. El uso de dispositivos móviles personales dentro de los penales está prohibido.

control de seguridad, con lo que se manifiesta una ponderación por parte del legislador entre el derecho a la inviolabilidad de las comunicaciones y la seguridad pública, máxime si en Perú el mayor porcentaje de los delitos de extorsión, secuestro y robos son organizados en los Centros Penitenciarios, razón por la cual el artículo 37 del Reglamento de Código de Ejecución Penal, modificado en el año 2011, regula el ejercicio de este derecho de la siguiente manera:

> *"(…) implementará la instalación de teléfonos públicos exclusivamente en cabinas con accesos comunes en los establecimientos penitenciarios, excepto en los de Régimen Cerrado especial de máxima seguridad. (…) Dicho servicio telefónico público contará con un sistema de identificación de llamadas u otro mecanismos que permita a la Administración Penitenciaria obtener un reporte de las llamadas realizadas por los mismos internos, así como al receptor de las mismas, conocer el origen de donde provienen",*

Este mismo artículo establece la restricción de las telecomunicaciones diferentes a las permitidas por la Administración: "En consecuencia, se encuentra prohibido por parte de los internos el uso de cualquier otro servicio de telecomunicaciones que permita la transmisión de voz y/o datos, distinto a los teléfonos públicos y locutorios instalados para tal efecto". En este sentido, las telecomunicaciones de los internos son controladas por fines de seguridad pero no se puede realizar una interceptación sin un permiso judicial.

3.3. Caso español en la interceptación telefónica legal para enfrentar el terrorismo

La Constitución española establece que los reos durante el cumplimiento de su pena tienen acceso a la comunicación, a través de los teléfonos fijos de los penales por ejemplo, puesto que a través de las comunicaciones los reclusos no se ven reducidos al mundo carcelario y pueden relacionarse con el exterior.

El marco jurídico español para la interceptación telefónica legal dentro de los centros penitenciarios determina que el acuerdo intervención debe ser motivado. En tal caso se requiere de una resolución con referencia de hechos y fundamentos de derecho en conjunto a razones materiales o indicios objetivos que establezcan el motivo por el cual se requiere de la intervención a la comunicación del reo. La sentencia del Tribunal Constitucional 170/1996 de 29 de octubre declara que:

> "el artículo 51 LOGP sólo legitima la restricción del derecho al secreto de las comunicaciones en cuanto concurran y perduren las razones que justifican o justificaron en su día la adopción. De ahí, la importancia de la motivación del acuerdo de intervención, no sólo porque así lo exige el art. 51 LOGP, sino porque constituye el único medio para constatar que la limitada esfera jurídica del ciudadano interno en un Centro Penitenciario, no se restringe o menoscaba de forma innecesaria, inadecuada o excesiva".

En particular, en lo que refiere a los casos de terrorismo, en España el Ministro del Interior o el Director de la Seguridad

del Estado pueden autorizar intervenciones y escuchas de las comunicaciones para realizar investigaciones.[71] Es necesario que se remita tal decisión inmediatamente por escrito al juez competente quien, de forma escrita, revocará o confirmará la resolución durante un plazo de máximo setenta y dos horas desde que se realizó la orden de observación.

Ya se ha visto que otros países, del mismo modo, tienen complejos sistemas de espionaje y escuchas:

> "Al complejo de espionaje más desarrollado existente actualmente dedicado a la interceptación de las comunicaciones electrónicas a nivel de todo el globo terráqueo (…) se le conoce como *Echelon*. Esta red, controlada por los Estados Unidos y que comparte parcialmente con sus aliados, controla diariamente más de tres mil doscientos millones de comunicaciones (…)."[72]

En el 2015 el Ministerio del Interior español aprobó una gran inversión en un sistema de interceptación de comunicaciones de personas sospechosas en tiempo real. El sistema se llama "Evident X-Stream" y para el 2017 se espera que la empresa adjudicada, BAE Systems, lo tenga operativo.[73] Con tal contrato los sistemas podrán modernizarse y será posible controlar en tiempo real la mayoría de comunicaciones de un individuo.

---

71 Cfr. La información. *Así son las leyes antiterroristas de Europa: en Reino Unido, las más duras*. Noviembre, 2015. http://noticias.lainformacion.com/disturbios-conflictos-y-guerra/terrorismo/asi-son-las-leyes-antiterroristas-de-europa-en-reino-unido-las-mas-duras_xUYxl5T8dS8djSdyDNnyE/ (última visita: 15 de mayo, 2016).

72 LOSADA, Juan Carlos. *De la honda a los drones*. Barcelona, 2014, p. 307.

73 Cfr. PALAZUELOS, Félix. *El plan del Ministerio de Interior español para interceptar las comunicaciones terroristas*. Diciembre, 2015. http://hipertextual.com/2015/12/ministerio-del-interior-comunicaciones-terroristas (última visita: 15 de mayo, 2016).

El sistema funciona de tal manera que se pueda mantener un seguimiento del ordenador o Smartphone del objetivo donde se podrán interceptar diferentes vías de comunicación como llamadas telefónicas, SMS, fotos, descargas, visitas de páginas webs, entre otros. El mayor problema serían las comunicaciones cifradas ya que complican traspasar los cuerpos de seguridad al ser difíciles de descifrar.

Con el nuevo sistema se hace uso de toda la información que se puede obtener de un teléfono como su geolocalización a través del historial de coordenadas o aviso y escucha de llamadas entrantes. El objetivo es obtener información para que a partir de la misma se pueda abrir una investigación con más recursos dado que con el sistema se pueden elaborar informes sobre todos los registros del investigado con lo cual el juez competente pueda solicitar su detención con una mayor rapidez.[74]

3.3.1. Propuesta para el caso peruano dentro de la ley

La propuesta, para el caso peruano dentro de la ley, refiere a la formación de inteligencia que pueda ser utilizada para la lucha activa contra la delincuencia y el crimen organizado, especialmente el narcotráfico y terrorismo en un esquema de lucha de una 4WG.

Pedro Tolentino[75], quien trabajó durante 10 años en el Servicio

74 Cfr. *Ídem.*
75 Ver Anexo 1.

de Inteligencia (SIN), considera que en una primera instancia es fundamental la capacitación de los agentes y trabajadores dado que el avance de la tecnología es constante. Es medular que se produzca una actualización constante de aprendizaje para poder captar y analizar los blancos. En especial, destaca que "un agente de inteligencia no se forma de la noche a la mañana, es a largo plazo para que adquiera experiencia y tenacidad".

Por ello es que en el campo de la Inteligencia Electrónica (OSINT)[76], el agente que realiza las escuchas tiene un rol importante al ser el primero en evaluar y direccionar el trabajo del entorno del blanco. Tolentino con ello asegura que "los resultados en el campo de Inteligencia Electrónica, no tienen límite, pueden ser a mediano o largo plazo, lo más importante es no perder el blanco y seguirlo". Es así que el trabajo da resultados: "en el campo de la lucha contra el narcotráfico se pudieron detectar varias organizaciones de narcotraficantes las cuales fueron detenidas por la DIRANDRO y puestas a disposición de la justicia."

En un inicio el SIN tenía la misión de dedicarse exclusivamente a la lucha contra el narcotráfico. A pesar de ello, debido a que con el equipo de Inteligencia Electrónica se pudo detectar información muy importante, el SIN ordenó enviar equipo de Inteligencia Electrónica para obtener información que fluía dentro de los penales, tal y como el de Castro Castro y

76 Cfr. *Ídem. (Anexo 1)*

Lurigancho. Con ello se obtuvo "una amplia información al respecto porque los delincuentes usan celulares, con jergas propios de su argot, donde se mensajean para perpetrar sus actos criminales."

Fue de este modo que la Comunidad de Inteligencia, durante 1998 y 1999, logró capturar bandas criminales y el gobierno tuvo acciones contundentes al respecto. A partir de ello es que la Comunidad de Inteligencia en la lucha contra la delincuencia requiere de equipos de Inteligencia Electrónica (Escuchas). Tolentino, además, considera que la incorporación de bloqueadores en los penales por parte del gobierno es un grave error puesto que "hoy la Comunidad de Inteligencia necesita información de fuente A1 para la lucha contra la delincuencia y sicariato; por ello es un grave error bloquear el flujo de información que pueden proporcionar los delincuentes detenidos en los diferentes penales."

El éxito de las operaciones se da por el flujo de información que proporcionan los equipos de Inteligencia Electrónica; dentro de los penales hay un gran flujo de información por parte de integrantes de bandas criminales por lo cual el gobierno debería, bajo una política de Estado, implementar equipos de Inteligencia Electrónica para lograr desarticular la delincuencia criminal donde podría anticiparse a la acción de reglaje, secuestro, sicariato, narcotráfico, entre otros crímenes.

CONCLUSIONES

1. A través de la elaboración de inteligencia es posible enfrentar efectivamente al crimen organizado, narcotráfico, terrorismo y sicariato, al tratarse de un producto que contrasta las diferentes opciones de acción. De forma tal, que el acceso a la información, es de vital importancia al ser el insumo básico de inteligencia. Su bloqueo y/o eliminación es un grave error.

2. El permanente contrabando de tecnología en las prisiones lleva a que estos centros de reformación se conviertan en lugares de ideologización criminal donde los reos siguen interactuando con el exterior y tienen la posibilidad de cometer crímenes.

3. El bloqueo de señales es un simple facilismo, ya que mantiene la filtración de la información en los penales; con lo cual se siguen cometiendo diversos delitos dentro y fuera de los mismos y además perjudica a las personas que viven en zonas adyacentes a los establecimientos penitenciarios, al tener un campo de acción mayor al área del propio penal. Es iluso pretender que los internos coordinen sus acciones criminales a través de los teléfonos de uso público instalados por el INPE, ya que estarían siendo conscientes de la interceptación de sus comunicaciones y el seguimiento de sus teléfonos de contacto.

4. Los inhibidores de señal no evitan la filtración de información y comunicación que se da entre los reclusos y sus abogados o familiares, por lo que hay un flujo de información que no puede ser interceptado ni utilizado para la elaboración de inteligencia.

5. Las escuchas de comunicación telefónica legal (presencia de fiscal ad hoc y autorización de juez competente) deben tener como propósito que la información obtenida y procesada por analistas de inteligencia, son de interés público y están destinadas para el bien común de la sociedad en las acciones integrales de confrontación de la 4WG. Para ello la DINI cuenta con equipos de última generación.

6. Dentro de los penales, especialmente de máxima seguridad, hay un gran flujo de información por parte de integrantes de bandas criminales por lo cual el gobierno debería implementar equipos de Inteligencia Electrónica, dentro del marco legal vigente, para lograr desarticular la delincuencia criminal.

Bibliografía

AGUSTINA SANLLEHÍ, José R. *El debate actual entre privacidad y prevención del delito: una propuesta comunitarista.* InDret, revista para el análisis del derecho. Barcelona, 2010.

ARGANDOÑA, Antonio. *El bien común*. Barcelona, 2011.

California Council on Science and Technology (CCST). *The Efficacy of Managed Access Systems to Intercept Calls from Contraband Cell Phones in California Prisons.* Sacramento, 2012.

Comisión Episcopal de Acción Social (CEAS). *Perú: Informe sobre la situación Penitenciaria.* Lima, 2005.

DE LA CORTE IBÁÑEZ, Luis y BLANCO NAVARRO, José María, et. al. *Seguridad nacional, amenazas y respuestas.* Lid Editorial Empresarial. España, 2014.

Defensoría del Pueblo. *El sistema penitenciario: componente clave de la seguridad política criminal. Problemas, retos y perspectivas.* Lima, 2011.

DÍAZ FERNÁNDEZ, Antonio M. (Dir.) *Diccionario LID. Inteligencia y seguridad.* Lid Editorial Empresarial. España, 2013.

El Comercio. *INPE incautó 387 celulares y droga en el penal Castro Castro.* Junio, 2015. http://elcomercio.pe/lima/ciudad/penal-lurigancho-presos-tienen-piscinas-y-discotecas-noticia-1825414 (última visita: 21 de marzo, 2016).

El Comercio. *Penal de Lurigancho: presos tienen piscinas y discotecas.* Julio, 2015. http://elcomercio.pe/lima/ciudad/penal-lurigancho-presos-tienen-piscinas-y-discotecas-noticia-1825414 (última visita: 21 de marzo, 2016).

El Comercio. *Preso de la banda de 'Caracol' lanza amenazas vía Facebook.* Enero, 2016. http://elcomercio.pe/lima/ciudad/penal-lurigancho-presos-tienen-piscinas-y-discotecas-noticia-1825414 (última visita: 21 de marzo, 2016).

Enforcement Bureau. *GPS, Wi-Fi, and Cell Phone Jammers Frequently Asked Questions (FAQs)*. FCC, http://transition.fcc.gov/eb/jammerenforcement/jamfaq.pdf (última visita: 20 de marzo, 2016).

Escuela de Inteligencia Nacional (ESIN). *Manual de inteligencia estratégica del SINA. Aspectos básicos y comunes a todos los campos. Tomo I.* ESIN. Lima, 1997.

FITZGERALD, Erin. *Cell 'Block' Silence: Why Contraband Cellular Telephone Use in Prisons Warrants Federal Legislation to Allow Jamming Technology*. Wisconsin, Law Review. Wisconsin, 2010.

GSM Association (GSMA). *Common position proposal on signal inhibitors (jammers) in Latin America.* 2014**. GONZÁLES CUSSAC, José Luis (coord.).** *Inteligencia.* Tirant Lo Blanch. Valencia, 2012.

Instituto Nacional Penitenciario (INPE). *Informe estadístico penitenciario.* Ministerio de Justicia y Derechos Humanos. Perú, 2015.

KISSINGER, Henry. *Orden Mundial. Reflexiones sobre el carácter de las naciones y el curso de la historia*. España, 2016.

LOSADA, Juan Carlos. *De la honda a los drones*. Barcelona, 2014

La información. *Así son las leyes antiterroristas de Europa: en Reino Unido, las más duras*. Noviembre, 2015. http://noticias.lainformacion.com/disturbios-conflictos-y-guerra/terrorismo/asi-son-las-leyes-antiterroristas-de-europa-en-reino-unido-las-mas-duras_xUYxl5T8dS8djSdyDNnyE/ (última visita: 15 de mayo, 2016).

MARCIANI BURGOS, Betzabé. *Interceptaciones telefónicas ilícitas, vida privada e interés público. O las marchas y contramarchas del Tribunal Constitucional en relación con la libertad de expresión de los medios de comunicación*. Instituto de defensa Legal – Justicia Viva. España, 2010.

MARTÍNEZ GÓMEZ, J.A. *El poder, el bien común y los intereses individuales y sociales*. Contribuciones a las Ciencias Sociales. 2011.

PALAZUELOS, Félix. *El plan del Ministerio de Interior español para interceptar las comunicaciones terroristas*. Diciembre, 2015. http://hipertextual.com/2015/12/ministerio-del-interior-comunicaciones-terroristas (última visita: 15 de mayo, 2016).

Pontificio Consejo Justicia y Paz. *Compendio de Doctrina Social de la* Iglesia. Librería Editorial Vaticana. Ciudad del Vaticano, 2005.

POOLE, Diego. *Bien común y derechos humanos*. Persona y derecho: Revista de fundamentación de las Instituciones Jurídicas y de Derechos Humanos. 2008, N° 58, pp. 97-134.

PORADA, V. et. al. *Environmental safety. Security in 21st Century.* Actas de la Universidad Politécnica de Odessa, 2013.

RÉNIQUE, José Luis. *La voluntad encarcelada. Las 'luminosas trincheras de combate' de Sendero Luminoso del Perú.* Texas, 2003.

"Shining a light in the Darkness of Peru's Prisons". Interview with Comrade Inez. *World To Win*, 1999, N° 25.

The National Telecommunications and Information Administration (NTIA). Contraband cell phones in prisons: Possible Wireless Technology Solutions. 2010.

Anexo 1

Rol de preguntas a integrante grupo de inteligencia del SIN año 90 al 2000

Dígame por favor sus generales de Ley

Mi nombre es Pedro Jaime Tolentino García, Técnico de Primera Ejército Peruano, Egresado de la Escuela Superior Técnica del Ejército 1986, vivo en Surco Lima Perú.

¿Cuánto tiempo laboró usted en el Servicio de Inteligencia SIN?

Trabajé en el SIN diez años.

¿Diga usted en qué año trabajó en el Servicio de Inteligencia Nacional SIN y cuál fue su trabajo o cargo?

Llegué a trabajar al SIN en febrero del año 1990 hasta su desactivación en noviembre del año 2000. Inicialmente tuve el cargo de escucha (interceptación de señales o interceptación

radio), el cual consistía en captar las señales de radio en frecuencia abierta, donde se transmitían por parte de la Policía y entidades del gobierno acciones de noticias de fuente abierta. Luego por el año de 1992 cuando se logra un convenio con el gobierno de Estados Unidos para la lucha contra el narcotráfico pasé a hacerme cargo de la administración de la red informática así como a integrar un equipo de escucha de celulares para la lucha contra el narcotráfico.

¿Cuál fue su experiencia en el campo de inteligencia en el uso de equipos para escucha de celulares en el SIN?

Como verá, en los años 90 se inicia en el Perú el uso masivo de celulares a nivel nacional, siendo primero señales analógicas y luego pasando a señal digital hasta la actualidad que es señal 4G. Ello fue un medio de comunicación, en los primeros años, al alcance de personas con poder económico.

El Servicio de Inteligencia SIN, mediante el ploteo (interceptación y evaluación) de señal de radio frecuencia y los análisis de la información que fluía, llegó a la conclusión de que los narcotraficantes estaban migrando su comunicación a la vía celular. Por ello fue importante el aceptar, como parte del convenio anti drogas, equipos de escucha celular del gobierno estadounidense para el trabajo de Inteligencia Electrónica.

La comunicación inicial de los narcotraficantes vía celular fue masiva, al punto que no cuidaban el dar detalles de sus operaciones. El trabajo de campo en esos primeros años de uso de equipo era arriesgado porque se hacía estando muy cerca del blanco ya que el alcance de los equipos de escucha era muy limitado. En la actualidad, los equipos son más sofisticados y sus limitaciones son de carácter legal.

¿Quiere decir que el Servicio de Inteligencia SIN a usted lo preparó intelectualmente para el trabajo de campo?

Sí, en los primeros años de servicio en el SIN recibí capacitación en el extranjero para el uso y explotación de equipos de Inteligencia Electrónica (escucha). La capacitación era constante debido al continuo avance de la tecnología y medios para captar y analizar blancos. Un agente de inteligencia no se forma de la noche a la mañana, es a a largo plazo para que adquiera experiencia y tenacidad.

¿Cuál fue su experiencia en el uso de equipo de escucha de señal electrónica durante el tiempo que usted trabajó en el Servicio de Inteligencia (SIN)?

En el campo de la Inteligencia Electrónica el agente de escucha, juega un papel muy importante, es el primero en evaluar y direccionar el trabajo del entorno del blanco. Bajo esta primicia debo decir que inicialmente fue algo novedoso. Los resultados

en el campo de Inteligencia Electrónica no tienen límite, pueden ser a mediano o largo plazo, lo más importante es no perder el blanco y seguirlo.

El trabajo dio sus resultados, en el campo de la lucha contra el narcotráfico se pudieron detectar varias organizaciones de narcotraficantes las cuales fueron detenidas por la DIRANDRO y puestas a disposición de la Justicia.

En uno de los casos más relevantes tuvimos que seguir un blanco, un narco joven. Por las características del equipo, el seguimiento tenía que realizarse de cerca; ello dio como resultado que el blanco se diera cuenta de dicho seguimiento, a tal extremo que se puso en peligro la vida de dos agentes quienes fueron interceptados por dicho narco. Otro caso, que fue el inicio del éxito, fue la captura del narco Boris Foguel en Panamá. El trabajo de ubicación, seguimiento y captura estuvo liderado por un grupo de agentes del SIN en conjunto a la Policía Judicial de Panamá. Ambos casos se dieron gracias al trabajo del equipo de Inteligencia Electrónica.

Tras el convenio firmado con el gobierno americano, el SIN tenía como misión y dedicación exclusiva la lucha contra el narcotráfico. Sin embargo, a raíz de las escuchas que realizaba el equipo de Inteligencia Electrónica, y luego de pasar por el equipo de análisis, se detectó información muy importante en el año 1998, cuando entre las bandas criminales aumentó el

secuestro a empresarios. Tras la información obtenida, el SIN ordenó enviar equipo de Inteligencia Electrónica para adquirir información que fluía dentro de los penales tales como el Castro Castro y Lurigancho. Con ello se obtuvo una amplia información al respecto, porque los delincuentes usan celulares, con jergas propios de su argot, donde se mensajean para perpetrar sus actos criminales.

La Comunidad de Inteligencia logró en los años 1998 y 1999 capturar bandas criminales y el gobierno, con acciones contundentes (como darle la máxima pena al jefe de banda), permitió que los secuestros se redujeran.

Tras sus experiencias narradas, ¿podríamos decir que en la lucha contra la delincuencia la Comunidad de Inteligencia necesita contar con equipos de Inteligencia Electrónica (Escuchas)?

Claro que es muy importante que la Comunidad de Inteligencia cuente con equipos de Inteligencia Electrónica (escuchas) para la lucha contra la delincuencia que hoy en el Perú avanza descontroladamente.

¿Cómo ve usted que el gobierno de hoy esté poniendo bloqueadores (inhibidores de señal) en los penales?

Hoy la Comunidad de Inteligencia necesita información de fuente A1 para la lucha contra la delincuencia y sicariato;

por ello es un grave error bloquear el flujo de información que pueden proporcionar los delincuentes detenidos en los diferentes penales. Se debe tener una estrategia para que equipos de Inteligencia Electrónica exploten al máximo el flujo de información que puedan proporcionar tanto los jefes de bandas como delincuentes.

Es necesario, bajo supervisión, que los delincuentes crean que están burlando a la Justicia al ingresar a los penales celulares. El éxito de una operación se da por el flujo de información que proporcionan los equipos de Inteligencia Electrónica, que es un 90% de la operación, lo otro es la parte operacional. Es un grave error que el gobierno, por cuestiones políticas y presiones mediáticas, opte por lo más fácil: poner bloqueadores en los penales.

¿Cuál sería el beneficio para la comunidad de inteligencia el que no bloquen los celulares en los penales?

Hoy tras muchas capturas de delincuentes por parte de la policía que purgan penas en los penales, el flujo de información que puede estar flotando en los penales para explotar y lograr capturar a todos los integrantes de una banda criminal es fuerte. Por ello sería muy importante que el gobierno, bajo una política de Estado, implemente equipos de inteligencia electrónica para lograr desarticular planes de los criminales, anticipándose a la acción de reglaje, secuestro, sicariato y otros crímenes.

Anexo 2

Ubicación geográfica de los Establecimientos Penitenciarios en el territorio peruano

Anexo 3

Hacinamiento y piscinas en el E.P. Lurigancho (Lima)