ESCPOGRA PNP

REVISTA ACADÉMICA DE LA ESCUELA DE POSTGRADO DE LA POLICIA NACIONAL DEL PERÚ

Edición especial 2024

2024/Año 1/N°1

ESCUELA DE POSGRADO

POLICIA NACIONAL DEL PERU

DIOS PATRIA LEY

DIRECTORIO

Esta Revista Académica de la Escuela de Posgrado de la Policía Nacional del Perú, es una publicación especial de carácter académico.

Los artículos presentados expresan el punto de vista de sus autores y la revista no se solidariza necesariamente con ellos.

Revista Académica Escpogra PNP
https://revistapograpnp.com/ojs/index.php/1/about
ISSN: 2961-2527 (En línea)

PRESENTACIÓN

DIRECTOR DE LA ESCUELA DE POSGRADO DE LA POLICÍA NACIONAL DEL PERÚ
Coronel PNP Miguel Ángel Mesta Rebaza

La Revista Académica ESCPOGRA PNP, es el medio por excelencia para hacer visisble los resultados de la investigación académica, nuestra Revista publica artículos y colaboraciones que forman parte del accionar policial, producto de las actividades académicas científicas que sirven como insumo para generar nuevos conocimientos basados en evidencias. La revista académica forma parte del repositorio del conocimiento policial de acceso libre, lo cual permite generar un espacio de interacción con los conocimientos policiales.

La Revista Académica ESCPOGRA PNP, se encuentra indizada en 7 bases de datos a nivel internacional como lo es LatinREV, Academic Resource Index, DRJI, Latino Americana, EuroPub, LivRe, Semantic Scholar y se encuentra inscrita en el directorio de Latindex y tiene como objetivo brindar conocimientos sobre temáticas policiales desarrolladas por la comunidad policial. En esta edición especial se publican 6 artículos académicos emitidos en los 3 últimos números publicados en formato virtual.

CONTENIDOS

Prólogo

La presente publicación representa el trabajo académico realizado de los oficiales PNP egresados, docentes y civiles administrativos de la Escuela de Posgrado Policía Nacional del Perú. En esta primera edición impresa se muestran seis artículos con información actualizada, que representan no solamente una problemática, sino también aspectos teóricos que puedan servir a nuestros lectores para conocer la realidad problemática o como antecedente para futuros estudios.

La revista académica ESCPOGRA PNP publica artículos y colaboraciones vinculados al que hacer policial, principalmente, que son producto de las actividades académicas científicas que sirven como insumo para generar nuevos conocimientos basados en evidencias.

La revista tiene como Número Internacional Normalizado de Publicaciones Seriadas inscrita en la Biblioteca Nacional del Perú (ISSN por sus siglas en inglés): 29612527, efectúa sus convocatorias y publicaciones de forma electrónica, con una periodicidad semestral (dos números: enero - julio y agosto - diciembre), las cuales son abiertas al público en general y que viabilizan el proceso de recepción, evaluación, aprobación y publicación de artículos originales e inéditos en español, inglés y portugués sobre temas que se encuentran dentro de las líneas de investigación preestablecidas, los mismos que tienen el objetivo de contribuir a potenciar las competencias de nuestros lectores, sobre determinados fenómenos sociales o aspectos de nuestra realidad actual. Nuestra revista en su versión digital puede leerse en el enlace https://revistaescpograpnp.com/ojs/index.php/1/about.

La revista es de acceso libre, lo cual permite generar un espacio de interacción sobre fenómenos sociales vinculados a aspectos policiales, principalmente. En la actualidad, la revista académica ESCPOGRA PNP se encuentra indexada en bases de datos internacionales y el directorio de Latindex, lo cual permite que los artículos académicos que se publican en nuestra revista puedan ser leídos en todo el mundo.

Para garantizar la rigurosidad y calidad, el proceso editorial de la Revista aplica la revisión por pares ciegos (blind peer-review), que responden a los criterios de pertinencia, relevancia, originalidad, responsabilidad y aporte a la comunidad científica-académica, así como cumplir con los principios éticos propios de la investigación y que profesa nuestra institución.

Área de Investigación
ESCPOGRA PNP

Fraude informático en la modalidad de phishing en Lima

Pierre Ruiz Contreras

César Solís-Castillo

Escuela de Posgrado de la Policía Nacional del Perú

Introducción

En los últimos años, el Perú ha impulsado el desarrollo de infraestructura digital para potenciar la cobertura de Internet y el comercio digital; estás acciones requieren implementar nuevos servicios tecnológicos. Esta situación, según Guerrero y Quinde (2011), constituye una evidencia del crecimiento exponencial de las Tecnologías de Información y Comunicación que contribuyen al progreso humano, generando nuevas oportunidades para los ciudadanos, incluidos los ciberdelincuentes Al respecto, Alvarado (2018) advierte sobre la amenaza que representan los ataques cibernéticos, indicando que la sofisticación de las herramientas digitales ha transformado los métodos delictivos tradicionales; este desafío se refleja en cifras alarmantes, como los 3,946 casos de ciberdelitos reportados en 2022 por la División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú.

La ciberdelincuencia se caracteriza por su aparente anonimato (Acurio, 2016). Se ha perfeccionado con el tiempo, dificultando su rastreo a pesar de los avances en tecnología forense (Nectec, 2018). Este fenómeno ha propiciado la estructuración de grupos criminales, que explotan las ventajas del Internet para perpetrar sus actividades ilícitas, generando múltiples desafíos para la persecución del delito (Jiménez, 2005). Por lo tanto, abordar esta problemática requiere una estructura conceptual respaldada en bases teóricas sólidas y evidencias.

La criminalidad cibernética adopta diversas modalidades, desde el hackeo hasta el robo de información personal (Gonzáles, 2017). El phishing es la técnica criminal que implica la creación de páginas web y la modificación de diseños de mensajería electrónica para simular legitimidad, que ha resultado en la obtención fraudulenta de contraseñas y otros datos sensibles por parte de los delincuentes (García, 2018). El primer ataque de phishing tuvo lugar a mediados de 1990, siendo objetivo la compañía estadounidense de servicios de Internet y medios, American Online-AOL (Flores, 2017).

En la actualidad, el delito ha evolucionado, adoptando nuevas estrategias por grupos criminales para engañar a usuarios. Diversos estudios, como los de Benavides et al. (2020), destacan que el phishing se realiza principalmente a través de la ingeniería social, con ataques orientados a la creación de páginas web adulteradas y el envío masivo de correos electrónicos fraudulentos. Por su parte, Alabdan (2020) destaca la importancia de la prevención ante el phishing, que es una preocupación global debido a su papel como principal generador de infecciones de malware y su uso como método de infiltración a través de técnicas de manipulación de datos.

Entre las formas de phishing, la suplantación de identidad representa una problemática de elevado interés. Al respecto, los hallazgos del estudio de la empresa Kaspersky señalaron que un 48,63% de la mensajería electrónica corresponde a spam, siendo el 52,78% de este spam de origen ruso, país al que se le atribuye un 29,82% de estos delitos (Kulikova y Dedenok, 2022). Por otra parte, el estudio de la empresa Comparitech reportó que se alcanzó un récord histórico en los años 2019 y 2022, reportando más de 300.000 ataques, que representan un incremento de hasta el 300% con respecto al año 2019 (Cook, 2023).

El delito informático en el Perú se refiere a conductas delictivas que hacen uso de las tecnologías y que afectan bienes jurídicos, descrita en la Ley 30096, conocida como «Ley de Delitos Informáticos», modificada por la Ley 30171. En este contexto, Gonzales (2022) sostiene que los investigadores deben orientarse hacia políticas claras y modelos policiales que permitan realizar análisis con recursos tecnológicos, lo cual contribuiría a la construcción de metodologías efectivas. Esta idea coincide con lo planteado por Cabero (2010), quien destaca la importancia de evolucionar para hacer frente al aumento de las necesidades y la problemática en este campo. La función de la policía consiste en garantizar, mantener y restablecer el orden interno, según lo establecido en el artículo 166 del Código Procesal Penal. En este sentido, Guillen (2011) considera que los encargados de afianzar la seguridad ciudadana deben aplicar políticas de justicia y llevar a cabo labores policiales efectivas. Por su parte, Gómez (2008) señala que la seguridad se logra mediante una política pública que organiza y estructura acciones para brindar servicios públicos que satisfagan las necesidades de los ciudadanos y aborden los problemas de inseguridad. Asimismo, Lopez et al. (2011) resaltan la importancia de las políticas públicas en la seguridad, aunado a la necesidad de adaptarse a las nuevas tendencias tecnológicas para enfrentar los problemas con eficacia y productividad (Iancu, 2016).

La medida adoptada por la Policía Nacional del Perú en el año 2005, mediante la Resolución Directoral No. 1695-2005-DIRGEN/EMG del 08 de agosto de 2005, fue la creación de la División de Investigación de Delitos de Alta Tecnología para la investigación de delitos mediante el uso de herramientas tecnológicas. En este contexto, el Mininter (2016) destaca el rol de los efectivos policiales de esta división en la recolección de evidencias digitales dejadas por los delincuentes, incluyendo modalidades como el phishing, una actividad delictiva en crecimiento que aprovecha la facilidad de acceso y uso de la tecnología para ocultar la identidad y ubicación de los

ciberdelincuentes.

Pese a la implementación de la normativa y la División de Investigación de alta Tecnología, el Perú experimenta un aumento sustancial de delitos cometidos por ciberdelincuentes, lo que ha motivado la campaña «Únete contra el ciberdelito» para concientizar sobre la importancia de denunciar y combatir estas modalidades delictivas (Oficina de las Naciones Unidas contra la Droga y el Delito [UNODC] y Defensoría del Pueblo [DP], 2021). Al respecto, el estudio de Puelles (2014) señala como una de las causantes de este incremento a la falta de especialización en materia de investigación policial en delitos informáticos.

A nivel nacional, estudios como el de Nazario y Villanueva (2022) señalaron que la legislación en materia de delitos informáticos ha permitido una persecución eficiente y la sanción de estas conductas, reduciendo la impunidad. Sin embargo, Hidalgo y Solano (2021) indicaron deficiencias en la regulación penal que permiten cierta impunidad en delitos como el phishing.
Asimismo, Villegas (2021) reportó la existencia de limitaciones en la interpretación y aplicación de medidas de ciberseguridad y detección de phishing, evidenciando la necesidad de mejorar tanto en el ámbito teórico como práctico.

En este sentido, el objetivo de la presente investigación es analizar cómo se realiza el fraude informático en la modalidad de phishing, en la División de Investigación de Delitos de Alta Tecnología-Lima.

Método

Se ha propuesto un enfoque de investigación cualitativo, para reconstruir la realidad, descubrirla e interpretarla (Ñaupas et al., 2018). Se aplicó el diseño fenomenológico-hermenéutico para pormenorizar los aspectos esenciales de esta experiencia, otorgándole sentido e importancia (Fuster, 2019). La muestra estuvo conformada por 07 efectivos policiales de la unidad especializada donde se investiga este tipo de incidencia delictiva, considerando una porción significativa de la población, para lo cual se empleó el muestreo no probabilístico por conveniencia (Lumbreras, 2018).

Para poder recolectar la información, se utilizó la técnica de la entrevista para recoger las percepciones y experiencias de los participantes sobre el fenómeno de estudio (Bonilla y Rodríguez, 2005) y el análisis documental, por lo que se utilizó como instrumento la guía de entrevista semiestructurada, validada por juicio de expertos, y la ficha de análisis documental. Esta guía estuvo constituida por 12 preguntas, las 3 primeras responden en analizar cómo se realiza el phishing, otras 3 preguntas para conocer el phishing, las 3 siguientes para describir cómo se comete y las 3 últimas para describir las consecuencias.

Antes de iniciar la recolección de información, los participantes firmaron el consentimiento. Posteriormente, las entrevistas fueron trascritas, para luego ser organizadas y trabajadas en un Excel, cuyo análisis se realizó mediante la técnica del coloreo (Vivar et al., 2010), respondiendo a cada objetivo de investigación.

Resultados

Para responder al objetivo de investigación, se comete fraude en la modalidad de phishing, se trata de engañar a los usuarios para que compartan su información personal de números de tarjetas y contraseñas, realizando una pesca ilegal de datos a través de la remisión de mensajes de texto o correo electrónicos, que imitan ilegalmente a las páginas web oficiales.

En esta modalidad de fraude informático, los ciberdelincuentes envían correos electrónicos masivos a múltiples usuarios, los cuales contienen enlaces o un archivo que contiene virus troyano, que sirven de acceso a páginas web que están diseñadas de tal manera que aparentan o suplantan páginas de empresas o entidades bancarias, donde le solicitan al usuario datos bancarios como número de tarjeta, fecha de expiración, código CCI, clave de internet, DNI, teléfono y clave TOKEN; esto con la finalidad de poder acceder a sus cuentas personales y beneficiarse del patrimonio (Entrevistado 2, 4, 5, 6 y 7).

En cuanto a las herramientas más utilizadas para cometer el fraude en la modalidad de phishing, debido a la extensión y acceso a Internet, el correo electrónico se convierte en un medio tradicional para enviar mensajes de manera sencilla, particularmente para enviar enlaces peligrosos y/o que pongan en riesgo la información personal contenida en el ordenador.

El correo electrónico y los mensajes de texto

Corresponden a los servicios de mensajería y las redes que se utilizan por la elevada afluencia e interacción que permiten entre el ciberdelincuente y el usuario, que facilitan el secuestro de información. Al respecto se señaló: “son los mensajes fraudulentos de forma masiva, los servicios de correo electrónico de Gmail y Outlook (Hotmail), las redes sociales (Facebook, Instagram), el Ransomware y el Evelginx que captura los tokens de autenticación enviados como cookies” (Entrevistado 1).

El proceso del delito de phishing tiene como objetivo vulnerar la información del usuario, para lo cual se remiten correos maliciosos a tantos usuarios como sea posible (generalmente dirigidos a millones de usuarios), a quienes se pretende infectar sus equipos con un virus, el cual no busca atacar un sistema operativo, sino engañar al usuario, para que éste coloque información sensible de sus cuentas bancarias, la cual será utilizada por los criminales a través de transferencias ilícitas no reconocidas que ocasionan perjuicio económico.

Los ciberdelincuentes realizan un proceso de ingeniería social para elaborar, diseñar y suplantar páginas de empresas para obtener información importante y confidencial de sus víctimas mediante un link enviado de forma masiva; con dicha información los ciberdelincuentes ingresan a la verdadera página y hacen uso de los fondos o créditos de sus víctimas (Entrevistados 1, 3, 5 y 7).

Por otra parte, las personas que realizan fraude informático en la modalidad de phishing recurren a difundir enlaces fraudulentos, enviados masivamente, para obtener datos personales de los estados financieros. Por lo que, el medio de comunicación, correo electrónico, se convierte en herramienta de uso criminal. Al respecto, se evidenció que los medios para obtener información personal y sensible que permita realizar transferencias bancarias o chantajear a cambio de un beneficio económico (Entrevistados 1, 2, 4 y 7).

Con respecto a los tipos de phishing, se utilizan el envío de correos masivos, los ataques mediante un link, la mensajería instantánea, la suplantación de la página web de la entidad financiera, SIM doble y la mensajería personal. No obstante, se considera que existen dos tipos de phishing: i) Primero, referido al spam (la más sencilla y frecuente de las técnicas de phishing consiste en enviar un correo electrónico malicioso a millones de usuarios, pidiéndoles que introduzcan información personal), que puede realizarse por SMS, implica el envío de mensaje de manera masiva a cierto grupo de personas; en este caso se adjunta un enlace donde el agraviado accede, del cual lo redirecciona a un sitio web malicioso.

En (ii) segundo lugar, referido al ataque a grupos selectos, para lo cual recolectan información de la potencial víctima mediante la encriptación de archivos en un dispositivo, se emplea el Ransomware, que encripta los archivos de un dispositivo y niega a la víctima el acceso a ellos a menos que se pague un rescate (entrevistados 3, 6 y 7). Asimismo, se distingue el phishing de voz, que implica obtener información de cuentas bancarias a través del teléfono, utilizando como medio el engaño, la astucia y el ardid.

De esta manera, los fraudes se comenten a través de enlaces de sitios web, que aparentan ser tan reales que engañan al usuario, quien cree que navega por un sitio seguro para colocar información confidencial, la cual es sustraída por los ciberdelincuentes. Al respecto, los entrevistados indicaron: Se realiza de diferentes tipos, como el envío de correos electrónicos fraudulentos que dirigen a los clientes a páginas web falsas que aparentan a la de entidad bancaria, donde solicitan el número de tarjeta, DNI, contraseña de banca por Internet e incluso el código CVV; una vez obtenido la información realizan diferentes operaciones como transferencias, giros, compras por internet, retiros, entre otros; fraude que se concreta cuando se accede a los links recibidos por correos o enlaces (Entrevistado 1, 2 y 5).

Con respecto a cómo se detecta el fraude informático en la modalidad de phishing, en ocasiones resulta difícil reconocer, pero siempre existen las fallas ortográficas en la terminación del correo, la recepción de links de actualización de datos confidenciales, son formas de cómo detectar esta modalidad dado que ninguna entidad solicita datos confidenciales de sus clientes, es por ello que los entrevistados consideran que se puede detectar. Los entrevistados señalaron: la visualización de la nomenclatura del correo remitente, ya que en muchos casos solo varía una letra; si se recibe un email o un mensaje de texto, envían un enlace que llevará a una supuesta página del banco y solicitarán datos confidenciales (número de tarjeta, clave de Internet, clave de la tarjeta y el número de token); la página original, si se puede cambiar el código capcha (entrevistado 2, 4, 5 y 7).

Por otra parte, la modalidad más común en el fraude informático es la modalidad de phishing mediante el envío de un email; sin embargo, existen otras formas de mayor sofisticación. Al respecto se señaló: Los correos electrónicos que aparentan ser de la identidad bancaria y, utilizando el engaño, la astucia y el ardid, redireccionan a su víctima a un sitio web malicioso (Entrevistado 1, 2, 3, 5 y 7).

Las nuevas tecnologías favorecen al fraude informático en la modalidad de phishing, ya que permite el desarrollo, pero a la vez puede llevar a la ruina, y sobre todo si se cae en manos de los ciberdelincuentes, ya que no todos los usuarios están realmente preparados para reconocer un engaño o fraude con el uso de estas tecnologías. Sobre ello, se señaló: las entidades financieras son vulnerables, debido a que no cuentan con un buen sistema de seguridad que permita neutralizar estos delitos, aunado a la falta de conocimiento de los usuarios; en comparación, los atacantes se

actualizan para seguir con sus actos ilícitos (Entrevistados 3, 5, 6 y 7).

Con respecto a cómo se puede proteger el ciudadano del fraude informático en la modalidad de phishing, la forma de protegerse es a través de la comprobación de las direcciones web, observar las fallas ortográficas, no rellenar formularios a través del uso de correos electrónicos y no someterse a la presión del ciberdelincuente para la entrega de información confidencial. Puede ayudar a protegerse de esta modalidad que realiza ataques a diario, y el desconocimiento es el mejor aliado del ciberdelincuente. Al respecto, se señaló: No se debe brindar información confidencial por las páginas de entidades bancarias por Internet; las entidades financieras deben realizar campañas de prevención e informarle de los peligros de abrir cualquier mensaje a través del correo electrónico (Entrevistados 1, 3, 4 y 6).

Discusión de los resultados

La amenaza de esta modalidad no se asocia únicamente al envío de un link malicioso, sino al peligro que representa para la sociedad. Para vulnerar la información confidencial, esta situación fue descrita por García (2018) como la conducta delictiva que se basa en la utilización de los datos. Por lo tanto, las herramientas para la comisión de este delito se facilitan con el Internet, que permite la creación de sitios web falsos y remitir formularios mediante redes sociales que vulneren datos confidenciales de las personas (Benavides et al., 2020).

Los diversos servicios de mensajería sirven para poner en circulación los anzuelos que son retransmitidos a los miles de usuarios que hacen uso, por obligación o necesidad de realizar sus actividades, pero a la vez se colocan en el lado vulnerable, por eso esta modalidad es considerada como una preocupación global y vital en la actualidad, al ser principal generador de infecciones para infiltrarse (Alabdan, 2020).

El engaño para obtener información a través del Internet es parte fundamental de este proceso, puesto que el ciberdelincuente debe ingeniárselas para pescar esta información, que según Benavides et al. (2020) se obtiene con el uso de la ingeniería social, aprovechándose del desconocimiento del usuario o por curiosidad, siendo vulnerable a los ciberdelincuentes. Al respecto, Basit et al. (2021) sostienen que el uso de Internet facilita la obtención de datos confidenciales.

La tecnología no se detiene; siempre está evolucionando; hoy en día es fácil realizar pagos y obtener tarjetas bancarias desde la comodidad del usuario, pero este avance incide también en la aparición de nuevas modalidades delictivas que estudian la manera de cómo obtener información privilegiada para beneficiarse económicamente. El estudio de Nectec (2018) indica que los ciberdelincuentes han logrado constituir una profesionalización en su actuar criminal.

Se han reportado diversos tipos de phishing, como Whaling, Spear phishing, Pharming, el Smishing, “Phishing de voz”, “Spear phishing” o “lsmishing”, “Phishing por SMS”, “Ransomware”, “Whaling”, todos ellos con el único propósito el robo de información, como el número de tarjeta, clave de Internet y código de seguridad captcha, clave token y el código CVV, y disponer de ella a través de transferencias, giros, compras por Internet, retiros, entre otros, agraviando de esta manera económicamente a sus víctimas.

Esta situación se constituye como un tema de agenda para la sociedad, puesto que se exige a las instituciones de seguridad estrategias y/o acciones para detectar el fraude informático en

la modalidad de Phishing, para lo cual se puede optar por generar mecanismos preventivos para reconocer la nomenclatura del correo remitente, implementar prácticas en las entidades financieras para proteger información confidencial y elaborar sistemas y/o plataformas digitales confiables, fácilmente reconocibles por sus usuarios. Por lo tanto, se deben implementar políticas públicas enfocadas a la prevención y protección de información financiera en sitios web maliciosos (Lopez et al., 2011). Esto exige políticas públicas, con aras de frenar las nuevas amenazas.

Todo esto ha sido favorecido con la aparición de las nuevas tecnologías, las cuales han permitido el incremento de esta modalidad, sumado a la falta de seguridad de las instituciones bancarias, la falta de conocimiento de los usuarios, y la actualización de los ciberdelincuentes para seguir con sus actos ilícitos. Por ello, Alabdan (2020) indica que el fomento de la prevención busca generar el aumento de conciencia al ser una preocupación global en la actualidad.

Por otra parte, se debe enfatizar el fortalecimiento de la norma penal, que según Hidalgo y Solano (2021) no se permite incorporar de forma adecuada a los hechos fácticos del phishing. Asimismo, para Guillen (2011), se debe afianzar la seguridad ciudadana mediante una estrategia que articule la política de justicia y la labor de la policía. Finalmente, Gómez (2008) señala que la organización y la estructuración de acciones deben considerar como objetivo lograr satisfacer las necesidades de seguridad de los ciudadanos; esto se logra con la protección patrimonial y de la información bancaria y adopción de medidas de vigilancia y detección de operaciones fraudulentas, de manipulación o alteración de datos.

Conclusiones

La técnica del envío de correos electrónicos masivos a múltiples usuarios, para suplantar las páginas de entidades bancarias y acceder a la información confidencial que permita el control total para beneficiarse del patrimonio. Todo esto a través de la utilización de los datos, utilizando mensajes de texto, las diversas redes sociales y los servicios de correo electrónico, que en la actualidad es el principal generador de infecciones para infiltrarse.

El uso de la ingeniería social, los medios tecnológicos y el Internet sirven para obtener y secuestrar información personal y sensible que es utilizada por los ciberdelincuentes para aprovecharse del patrimonio de sus víctimas a través del chantaje o transferencias bancarias. Esta situación ha logrado una profesionalización en la forma de actuar, promovida por los valiosos ingresos económicos; por eso existen diferentes tipos de cómo realizar esta acción a través del Whaling, Spear phishing, Pharming, el Smishing, los links de correos electrónicos, Phishing de voz, Email/ Spam, Phishing por SMS, Ransomware y el Whaling.

El envío de correos electrónicos fraudulentos para obtener información confidencial, como el número de tarjeta, clave de internet, código de seguridad captcha y la clave token, les permite a los ciberdelincuentes realizar transferencias, giros, compras por internet, retiros, entre otros, agraviando de esta manera económicamente a sus víctimas, quienes desconocen la nomenclatura del correo remitente, la misma que debe ser revisada, ya que en muchos casos solo varía una letra, así como la verificación del código capcha.

El fraude informático se ha incrementado y se debe a la tecnología, los deficientes sistemas de seguridad de las diferentes entidades financieras, el desconocimiento de los usuarios y la actualización de los ciberdelincuentes para seguir con sus actos ilícitos. Esta situación ha generado

una preocupación global que requiere de campañas de prevención, mejorar el tipo penal, puesto que en la práctica se dificulta incorporar hechos facticos del phishing. Asimismo, la aplicación de la política de justicia y de la labor de la policía a la organización y la estructuración de acciones, con el único fin de satisfacer a los ciudadanos, quienes sufren el perjuicio patrimonial en cuestión de segundos, por el acceso a su información bancaria y las operaciones fraudulentas.

Referencias

Acurio, P. (2016). Delitos informáticos: Generalidades. EDIAR.

Alvarado, N. (2018). Tecnología contra el crimen: Entusiasmo con cautela y criterio. Banco Iberoamericano de Desarrollo. https://blogs.iadb.org/seguridadciudadana/es/tecnologia-contra-el-crimen-entusiasmo-con-criterio/

Benavides, E., Fuertes, W., y Sánchez, S. (2020). Caracterización de los ataques de phishing y técnicas para mitigarlos. Ataques: Una revisión sistemática de la literatura. Ciencia y Tecnología, 13(1), 97-104. https://doi.org/10.18779/cyt.v13i1.357

Bonilla, E., y Rodríguez, P. (2005). Más allá del dilema de los métodos. Ediciones Uniandes. https://laboratoriociudadut.files.wordpress.com/2018/05/mas-alla-del-dilema-de-losmetodos.pdf

Cabero, J. (2010). Los retos de la integración de las TICs en los procesos educativos: Límites y posibilidades. Perspectiva Educacional, 49(1), 32-61. https://dialnet.unirioja.es/servlet/articulo?codigo=3579891

Defensoría del Pueblo y Oficina de las Naciones Unidas Contra la Droga y el Delito (2021). Defensoría del Pueblo y la Oficina de Naciones Unidas contra la droga y el delito (UNODC) presentan campaña preventiva contra la ciberdelincuencia. DP y UNODC. https://www.defensoria.gob.pe/wp-content/uploads/2021/11/NP-1437-2021.pdf

Flores, C. (2017). El Phishing como comportamiento penalmente relevante. Valparaíso. Fondo de las Naciones Unidas para la Infancia. (2017). El estado mundial de la infancia 2017, Niños en un mundo digital. UNICEF. https://www.unicef.org/es/informes/El-Estado-Mundial-de-la-Infancia-2017

Fuster, D. (2019). Investigación cualitativa: Método fenomenológico hermenéutico. Propósitos y Representaciones, 7(1), 201. https://doi.org/10.20511/pyr2019.v7n1.267

García, D. (2018). El phishing como delito de estafa informática. Comentario a la SAP de Valencia 37/2017 de 25 de enero (rec. 1402/2016). Revista Boliviana de Derecho, 25, 650-659. https://dialnet.unirioja.es/servlet/articulo?codigo=6263417

Gómez, C. (2008). Elementos para la construcción de políticas públicas de seguridad ciudadana. Seguridad multidimensional en América Latina, 2008. FLACSO ECUADOR. https://www.flacsoandes.edu.ec/agora/elementos-para-la-construccion-de-politicaspublicas-de-seguridad-ciudadana

González, A. (2022, 10 de noviembre). Las nuevas tecnologías como apoyo a la labor policial, no como eje de la investigación. Universidad a Distancia de Madrid. https://www.udima.es/es/abel-gonzalez-polonia-nuevas-tecnologias-policia.html

González, M. (2017, 15 de noviembre). La cibercriminalidad como instrumento para la expansión yempoderamiento del crimen organizado. Grupo de Estudios en Seguridad Internacional. https://www.seguridadinternacional.es/?q=es/content/lacibercriminalidad-como-instrumento-para-la-expansi%C3%B3n-y-empoderamientodel-crimen

Guerrero, D., y Quinde, M. (2011). Las TIC en el Perú desde el desarrollo sostenible: una propuesta para las zonas rurales. XV Congreso Internacional de Ingeniería de proyectos - AEIPRO.

Guillen, F. (2011). Les polítiques de seguretat ciutadana [Las políticas de seguridad ciudadana]. Papers: Regió Metropolitana de Barcelona: Territori, estratègies, planejament, 1(53), 22-32. https://ddd.uab.cat/record/65474

Hidalgo, C., y Solano, G. (2021). El phishing como conducta delictiva no regulada en el ordenamiento jurídico peruano. Propuesta de incorporación del artículo 7-a en la Ley de Delitos Informáticos 30096 [Tesis de pregrado, Universidad Nacional del Santa]. https://hdl.handle.net/20.500.14278/3849

Huamán, M. (2020). Los delitos informáticos en Perú y la suscripción del Convenio de Budapest [Tesis de pregrado, Universidad Andina del Cusco]. https://hdl.handle.net/20.500.12557/4116

Iancu, A. (2016). Nuevas tecnologías, policía y prevención del delito [Tesis de Pregrado, Universitat Jaume I]. https://repositori.uji.es/xmlui/handle/10234/161486

Jiménez, R. (2005). La delincuencia juvenil: Fenómeno de la sociedad actual. Papeles de población, 11(43), 215-261. https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1405-74252005000100009

Kulikova, T., y Dedenok, S. (2022). El Spam y el phishing en 2022. SECURELIST. https://securelist.lat/spam-phishing-scam-report-2022/97582/

Lopez, S., Marchal, E., y Cuenca, M. (2011). Policía y seguridad pública de Pamplona. Editorial Aranzadi.

Lumbreras, B. (2018). Evaluación de los participantes en el proyecto: Productividad científica y capacidad investigadora. Quaderns de la Fundació Dr. Antoni Esteve, 1(43), 56-59. https://raco.cat/index.php/QuadernsFDAE/article/view/395608

Ministerio del Interior (2016). Ciberpolicías contra delitos informáticos. MINISTER. https://www.mininter.gob.pe/content/ciberpolic%C3%AD-contra-delitos-inform%C3%A1ticos

Nazario, N., y Villanueva, L. (2022). Fraude informático en la modalidad de phishing y la necesaria actualización de la legislación para una eficiente persecución y sanción penal

[Tesis de pregrado, Universidad Señor de Sipán]. https://hdl.handle.net/20.500.12802/10002

Nectec (2018). Nevil Maskelyne: El primer hacker de la historia. https://www.netec.com/post/nevil-maskelyne-el-primer-hacker-de-la-historia

Ñaupas, P., Valdivia, D., Palacios, V., y Romero, D. (2018). Metodología de la investigación Cuantitativa- Cualitativa y Redacción de la Tesis. Ediciones de la U.

Organización de las Naciones Unidas. (2019). El contexto y el diseño de TIC para el desarrollo mundial. United Nations - ONU. https://www.un.org/es/chronicle/article/el-contextoy-el-diseno-de-tic-para-el-desarrollo-mundial

Parada, R., y Errecaborde, J.(2018). Cibercrimen y delitos informáticos: Los nuevos tipos penales en la era de internet. Erreius. https://www.pensamientopenal.com.ar/system/files/2018/09/doctrina46963.pdf

Puelles, R. (2014). Luces y sombras de la delincuencia informática en Perú. Hiperderecho. https://hiperderecho.org/2014/07/luces-y-sombras-de-la-delincuencia-informaticaen-peru/

Villegas, J. (2021). Modelo de machine learning en la detección de sitios web phishing [Tesis doctoral, Universidad Señor de Sipán]. https://hdl.handle.net/20.500.12802/8897

Vivar, C., Solabarrieta, M., López, O., y Gordo, C. (2010). La Teoría Fundamentada: Como metodología de investigación cualitativa en enfermería. Index de enfermería: información bibliográfica, investigación y humanidades, 19(4), 283-288. https://dialnet.unirioja.es/servlet/articulo?codigo=3607354

La Importancia de la inteligencia táctica militar y policial en la producción de inteligencia estratégica nacional

Darwin José Mires Agip

Escuela de Posgrado de la Policía Nacional del Perú

Gonzalo Reyes Timana

Ministerio del Interior

Introducción

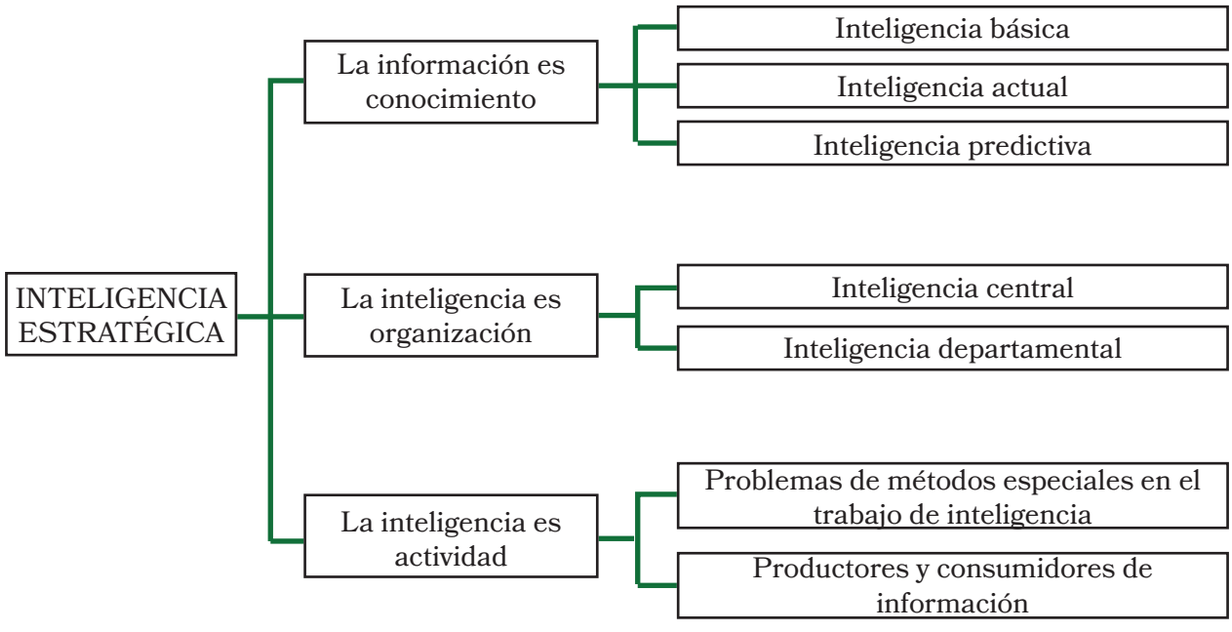
En un mundo en constante evolución, caracterizado por una creciente complejidad en materia de seguridad, geopolítica y geoestrategia, la capacidad de un país para tomar decisiones eficientes se vuelve un activo invaluable. En este contexto, la relación entre la inteligencia táctica y la inteligencia estratégica surge como elementos cruciales en el proceso de toma de decisiones a nivel nacional. De hecho, dentro del complejo entramado de la seguridad nacional y el análisis estratégico, la inteligencia táctica se revela como una herramienta fundamental para comprender y abordar los desafíos operativos inmediatos, mientras que la inteligencia estratégica se enfoca en identificar patrones a largo plazo y en la toma de decisiones a nivel macro. En este trabajo, se exploran los antecedentes de este tema en la comunidad de inteligencia, destacando el papel de la inteligencia táctica como piedra angular de las operaciones militares y policiales. También se aborda la importancia de la inteligencia estratégica nacional como conocimiento esencial para la toma de decisiones en los más altos niveles gubernamentales; examinando el vínculo entre la inteligencia táctica y estratégica, comprendiéndola como un círculo virtuoso productivo que potencia la toma de decisiones informadas.

Antecedentes en la comunidad de inteligencia

Durante la Segunda Guerra Mundial, la inteligencia estratégica alcanzó un nivel sin precedentes. Las naciones aliadas llevaron a cabo una exhaustiva recopilación y análisis de información para proporcionar conocimiento útil en la toma de decisiones a nivel gubernamental (Agencia Central de Inteligencia de Estados Unidos, 1981). Esto resultó fundamental para abordar los desafíos en el contexto bélico; tal situación destaca el papel crucial de la inteligencia estratégica, que alcanzó un nuevo horizonte gracias a las naciones que asignaron recursos significativos para orientar las decisiones estratégicas (Kent, 1966). Entre los referentes destacados en la comunidad de inteligencia se encuentra Sherman Kent, cuyo libro "Inteligencia Estratégica para la Política Mundial Norteamericana" popularizó la frase "La información es conocimiento y el conocimiento es poder".

Figura 1

Enfoques de la inteligencia estratégica.



Nota: Información obtenida del libro Inteligencia estratégica para la política mundial norteamericana de Kent (1966).

La información constituye la base del conocimiento. Según Kent (1966), la información representa la materia prima para generar inteligencia, específicamente, información extranjera de alto nivel que implica la correlación de datos. Este proceso es fundamental para la toma de decisiones, así como para la planificación y formulación de políticas y estrategias militares.

En este contexto, la inteligencia estratégica se define como el conjunto de conocimientos sobre países y organizaciones extranjeras. Su objetivo principal es respaldar la política exterior de un país, identificar oportunidades para la defensa de los intereses nacionales, anticipar posibles acciones de potencias adversarias, y contrarrestar políticas hostiles que puedan afectar las aspiraciones nacionales. Su función primordial es prevenir y alertar sobre amenazas y riesgos para la seguridad nacional.

Para desarrollar inteligencia estratégica, es importante distinguir entre dos tipos de información: la información de seguridad, asociada a la vigilancia y protección del país contra amenazas internas, y la

información positiva, que abarca aspectos de alta política extranjera y disposición de fuerzas enemigas, calificada como nivel estratégico.

Una vez diferenciados estos tipos de información, el proceso de obtención de conocimiento se divide en dos rutas: temática y funcional. El primero se centra en las políticas de Estado, incluyendo la política exterior y la seguridad nacional. El segundo aborda diversas facetas de la actividad humana que son relevantes para la producción de inteligencia estratégica, como la política, la economía, el entorno sociocultural, la identificación de actores clave y tendencias, la vigilancia de eventos relevantes, la formulación de problemas, la generación de supuestos e hipótesis, la aplicación de metodologías adecuadas, la capacidad para adoptar la perspectiva del adversario, y contar con personal capacitado para llevar a cabo estas labores de manera efectiva.

En cuanto a los tipos de información, se distinguen tres categorías principales. Primero, la información básica, que comprende datos descriptivos de tipo enciclopédico, como la geografía, población, economía, política y aspectos militares de los países de interés, con el propósito de tenerlas en archivo. Segundo, la información actual, que proporciona una visión de los cambios actuales y permite rastrear nuevas tendencias, modificaciones geográficas, económicas, militares, políticas, sociales, morales y científico-tecnológicas. Por último, la información predictiva, que surge del análisis especulativo-evaluativo para anticipar posibles cursos de acción en respuesta a estímulos externos.

La inteligencia se concibe como una organización que comparte recursos humanos y materiales, como personas, métodos, procedimientos, instalaciones y equipos, bajo una dirección y coordinación permanentes para lograr un objetivo (Kent, 1966). Se establece una analogía entre las organizaciones de inteligencia y las universidades, aunque con un ritmo más acelerado, siendo importante contar con personal que tenga la experiencia en investigación y el pensamiento riguroso arraigados como hábitos de vida, incluso aceptando la convivencia con individuos “extraños y excéntricos”, pero talentosos. Dado que esta organización está destinada a producir un producto (conocimiento) a partir de diversas materias primas y un trabajo competitivo, requiriéndose de normativas definidas y flexibles, así como de un ambiente laboral tranquilo y una biblioteca bien organizada.

El servicio de inteligencia debe reclutar y formar personal capacitado para llevar a cabo tareas de observación abierta, observación interior e investigación, utilizando canales de comunicación como “cables” que conecten la red. La inteligencia como organización se divide en inteligencia central, responsable de la coordinación y procesamiento de la información producida por diversos organismos, y la inteligencia departamental, encargada de obtener y producir inteligencia según sus competencias y áreas de interés específicas, como la inteligencia naval, aérea, militar, económica y social, evitando la duplicación de funciones en todo momento.

En el contexto peruano, la Dirección Nacional de Inteligencia (DINI), como entidad rectora del Sistema de Inteligencia Nacional (SINA), tiene la responsabilidad de generar inteligencia a través de diversos organismos de diferentes sectores. Estos incluyen el sector de Relaciones Exteriores, representado por la Dirección General de Asuntos Multilaterales y Globales; el sector de Defensa, que abarca la 2da Dirección de Estado Mayor Conjunto de las Fuerzas Armadas y las Direcciones de Inteligencia del Ejército, la Marina y la Fuerza Aérea; y el sector de Interior, con la Dirección General de Inteligencia del Ministerio del Interior y la Dirección de Inteligencia de la Policía Nacional del Perú. Estos organismos no solo producen inteligencia estratégica para sus respectivas instituciones y sectores, sino que también contribuyen con inteligencia en los ámbitos militar y policial para la elaboración de inteligencia estratégica a nivel nacional.

Según Kent (1966), estos tipos de organización no están exentos de presentar problemas, siendo el más frecuente el trabajo articulado, generalmente ocasionado por falta de coordinación y comunicación que afecta a la producción de inteligencia estratégica. Asimismo, la perseverancia de tales problemáticas ocasiona: conflictos de poder, confusión de competencias, duplicidad de funciones, falta de personal competente, control y supervisión exagerados, intromisión en la labor y afán de competitividad.

La actividad de inteligencia es continua e involucra a todos los organismos del sistema de inteligencia, cuyos procesos y métodos de investigación generan inteligencia estratégica. El inicio de la producción de este tipo de inteligencia está determinado por cambios en la política exterior, lo que mantiene alerta al sistema de inteligencia para observar las actividades del enemigo, adquirir conocimiento sobre sus capacidades y vulnerabilidades, y aproximarse a la verdad. Es fundamental señalar que la observación puede ser abierta, clandestina o una combinación de ambas, y su propósito es informar sobre las políticas o acciones de otros Estados que puedan afectar los intereses nacionales, así como proporcionar información relevante para guiar la política exterior propia. Este enfoque no busca obtener información superficial o esporádica, sino que a través de la investigación se genere información de calidad.

En cuanto al proceso de investigación, según Kent (1966), implica una metodología que abarca la identificación de un problema, su análisis, la recolección y evaluación de datos, el estudio de hipótesis, la confirmación o refutación de estas hipótesis mediante una mayor recolección de datos, la formulación de una o más hipótesis y su presentación. Esta dinámica entre productores y consumidores de información depende de la orientación clara y definición precisa del problema de seguridad, la claridad de los objetivos, la validez y aceptación de la información.

La inteligencia táctica como piedra angular de las operaciones militares y policiales

Las definiciones de inteligencia táctica y su importancia en los contextos militar y policial son cruciales para su entendimiento, según Sainz de la Peña (2012) se puede entender como “inteligencia positiva, extranjera” (p. 220), lo que implica la búsqueda de información a través de un proceso de indagación diligente; cuya evaluación e interpretación se realizan a partir de toda información disponible, incluyendo condiciones climáticas, geográficas y cualquier otra circunstancia relevante que influya en la toma de decisiones a nivel táctico sobre un enemigo real o potencial (Ordoñez y Cruz , 2017). A partir de ello, se pueden hacer deducciones sobre las capacidades actuales y futuras del enemigo, sus vulnerabilidades y sus probables formas de acción (Munar, 2010).

En el ámbito militar, la inteligencia táctica es fundamental para informar y orientar las decisiones operacionales, dado que implica la recopilación de información sobre los enemigos, así como la comprensión integral de las condiciones meteorológicas y el terreno. Esta perspectiva global brinda conocimiento a los líderes militares para prever los posibles cursos de acción del enemigo y prepararse para neutralizarlos (Ministerio de Defensa de España, 2003), lo que resulta de importancia para la toma de decisiones en situaciones de conflicto. Por su parte, la inteligencia táctica policial se centra en proporcionar conocimiento útil para la toma de decisiones en la prevención de delitos en tiempo real (Bogran et al., 2015) como principio básico para las operaciones policiales.

Inteligencia estratégica nacional, conocimiento esencial para la toma de decisiones en los más altos niveles gubernamentales

Según la normativa nacional, establecida en el marco del Decreto Legislativo N°1141 y sus modificatorias, la inteligencia estratégica desempeña un papel fundamental al proporcionar conocimientos relevantes para la toma de decisiones de la Presidencia de la República y el Consejo de Ministros. Este proceso permite la planificación y toma de decisiones en el más alto nivel gubernamental, abarcando diversas disciplinas, incluyendo los ámbitos militar y policial. Esta premisa se fundamenta en la historia de la humanidad, desde las civilizaciones antiguas hasta las naciones modernas, donde la recolección y análisis de información han sido pilares para formar una visión a largo plazo; esta importancia ha sido destacada por Sun Tzu en “El arte de la guerra”, al resaltar el papel crucial de la inteligencia en la estrategia (Tzu, 2021).

Por otro lado, la inteligencia estratégica también se define como el proceso de recopilación, análisis y aplicación de información para respaldar la toma de decisiones estratégicas (Hulnick, 2006). Puede abordar diversos aspectos, como geografía, política, legislación, economía, sociedad, tecnología, medio ambiente, entre otros, y se utiliza para evaluar y comprender el entorno competitivo en el que opera una organización

(Fuld, 1995). En el ámbito militar, este tipo de inteligencia se refiere a la información que contribuye a las decisiones a nivel nacional, en contraposición a la inteligencia táctica, que se emplea en el campo de batalla (Gearon, 2015). Por lo tanto, la inteligencia estratégica adquiere un valor como campo de estudio para la toma de decisiones informadas, que continúan siendo relevantes en el contexto moderno.

De esta manera, la generación de inteligencia estratégica a nivel país es esencial para comprender los desafíos y oportunidades que se afrontarán en el ámbito geopolítico y geoestratégico; sin embargo, no puede existir sin una sólida producción de inteligencia táctica, que proporcione información detallada sobre los actores, capacidades y actividades en el campo (Sainz de la Peña, 2012). Esta perspectiva es consistente con lo señalado por Zuñiga (2014) quien evidenció la importancia de lograr la articulación entre diversas instituciones de inteligencia, con el objetivo de mitigar la creciente desinformación, puesto que la información de inteligencia a nivel estratégico juega un papel fundamental para los Estados, ya sea para formular y ejecutar políticas públicas, y hacer frente a las amenazas a la seguridad procedentes del interior y exterior, las cuales son cada vez más complejas, difusas e interrelacionadas.

En un marco general, se destaca un creciente interés de la comunidad de inteligencia en las tecnologías de la información y comunicación, las redes sociales, la vigilancia tecnológica y la inteligencia artificial como herramientas para la investigación; si a ello se suma que la inteligencia táctica juega un papel crucial para la identificación de los detalles que trazan las nuevas tendencias, se obliga a su constante actualización a fin de que se vuelva cada vez más relevante y necesaria (Saavedra, 2016). Por ello, la forma de producir inteligencia táctica se ha ido adaptando a las nuevas realidades y amenazas emergentes; sin embargo, existe una brecha en torno al entendimiento de su importancia para la producción de inteligencia estratégica nacional.

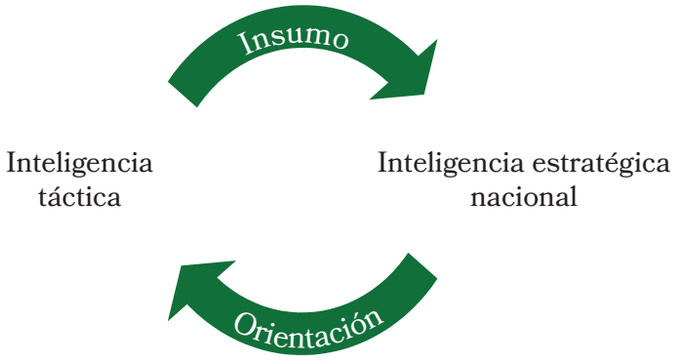
Vínculo entre la inteligencia táctica y estratégica, un círculo virtuoso productivo

La inteligencia táctica y estratégica son dos componentes interdependientes que desempeñan un papel fundamental en la seguridad nacional y en la toma de decisiones por parte de los responsables (Cabrera, 2016). La inteligencia táctica se enfoca en la recopilación y análisis detallado de información sobre actores, capacidades y actividades en el terreno, mientras que la inteligencia estratégica busca comprender los factores de riesgo, como causas estructurales, condiciones ambientales y eventos, así como identificar desafíos y oportunidades a largo plazo que puedan influir en la formulación de estrategias sociopolíticas.

La conexión entre ambas se establece a través de una relación de causa y efecto. La inteligencia táctica proporciona información detallada sobre la situación actual en el terreno, lo que permite comprender las capacidades y actividades de los actores, elementos fundamentales para la toma de decisiones estratégicas informadas. Por otro lado, la inteligencia estratégica nacional brinda una visión más amplia y a largo plazo, permitiendo identificar tendencias, amenazas emergentes y oportunidades. Esta información estratégica retroalimenta y orienta los esfuerzos de búsqueda para la producción de inteligencia táctica, al enfocar los recursos de recopilación y análisis en áreas pertinentes.

Figura 2

Círculo vicioso productivo entre los niveles de inteligencia.



Nota: Información obtenida que muestra la interacción entre los niveles de inteligencia.

Importancia de la inteligencia táctica para la producción de inteligencia estratégica

Contar con una sólida producción de inteligencia táctica ofrece múltiples beneficios para un país, considerando que se fundamente en el análisis de información obtenida de fuentes cerradas o secretas, lo que proporciona una base sólida de datos actualizados y precisos que contribuyen a evaluar las amenazas y oportunidades, y a desarrollar estrategias eficaces (De Miguel, 2021). Además, la inteligencia táctica ayuda a reducir la incertidumbre y proporciona una comprensión más clara de los actores y dinámicas en el terreno, siendo otro beneficio clave, su capacidad para anticipar y responder rápidamente a los eventos.

A nivel estatal, la inteligencia estratégica nacional es la encargada de advertir sobre amenazas y riesgos para la seguridad y defensa nacional, en línea con la Política Nacional Multisectorial de Seguridad y Defensa Nacional al 2030 (PNMSDN-2023) y el Plan Estratégico de Desarrollo Nacional al 2050 (PEDN-2050). Es fundamental cumplir con el artículo 17.2 del Decreto Legislativo 1141, que establece el fortalecimiento y modernización de la Dirección Nacional de Inteligencia (DINI) y el Sistema de Inteligencia Nacional (SINA). Este artículo señala la provisión de inteligencia estratégica al presidente de la República y al Consejo de Ministros para la formulación y ejecución de acciones y políticas destinadas a garantizar la vigencia de los derechos humanos, defender la soberanía nacional, promover el bienestar general y el desarrollo integral del país, así como proteger a la población de amenazas internas y externas contra su seguridad.

En el contexto actual, tanto internacional como nacional, se observa una interconexión sin precedentes debido a la disponibilidad y acceso a redes de comunicación y recursos digitales. La globalización ha generado una compleja red de relaciones entre naciones, economías y culturas, lo que implica que los acontecimientos en una parte del mundo puedan tener repercusiones significativas en otras regiones. Al mismo tiempo, la evolución tecnológica y la creciente accesibilidad a la información han transformado la dinámica política y social a nivel nacional. Desde esta perspectiva de interdependencia, los desafíos y oportunidades trascienden las fronteras, demandando una comprensión holística y una cooperación efectiva en todos los niveles (Zuñiga, 2014). Entre las principales características se presentan las siguientes:

Incremento en el flujo de la comunicación a través de las redes sociales. En la era digital, las redes sociales se han convertido en un canal de comunicación fundamental para las personas, empresas e instituciones del Estado; ya que proporcionan una plataforma en la que las organizaciones pueden interactuar directamente con su audiencia, compartir contenido relevante y recibir retroalimentación en tiempo real. El acceso a una audiencia global, la capacidad de segmentar y dirigir mensajes específicos ha impulsado un aumento significativo en el flujo de la comunicación a través de estas plataformas, que también son

utilizadas por los adversarios para acordar actividades y tareas específicas, en desmedro principalmente del orden público y la seguridad ciudadana.

Uso masivo de la inteligencia artificial (IA). Esta ha revolucionado la comunicación al automatizar tareas repetitivas, procesar y analizar grandes volúmenes de datos para extraer información relevante. Los chatbots basados en IA pueden proporcionar respuestas instantáneas a preguntas frecuentes y asistir en la elaboración de documentos. Asimismo, esta herramienta puede personalizar mensajes y recomendaciones en función de los perfiles y comportamientos que sean programados, en este escenario se hace necesario su conocimiento para advertir tendencias que sean producto de ella, las cuales puedan emplearse como apoyo a la producción de inteligencia.

Empleo de herramientas de *big data*. El uso de este tipo de herramientas ha permitido a las empresas analizar grandes volúmenes de datos generados por sus clientes y operaciones, incluir datos del escenario geográfico y analizar tendencias de información que permitan potenciar la producción de inteligencia táctica y adaptar enfoques de manera más precisa y eficaz para tales estrategias, así como establecer mapas de calor.

Inteligencia de negocios. Este tipo de inteligencia se utiliza en el ámbito empresarial, implica la recopilación, análisis y presentación de datos empresariales para tomar decisiones informadas. En el contexto de la comunicación empresarial, esto implica evaluar el rendimiento de las campañas de marketing, medir la efectividad de los canales de comunicación y ajustar las estrategias en consecuencia.En este campo, es preciso señalar que existen diversas ofertas educativas que pretenden aplicar la metodología del ciclo de producción de inteligencia estatal a los negocios.

Vigilancia tecnológica. Esta es un tipo de inteligencia que implica el seguimiento constante de las tendencias tecnológicas relevantes para una industria, la ciencia, así como la investigación, desarrollo e innovación (I+D+i). En el ámbito de la comunicación empresarial, permite a las empresas estar al tanto de las nuevas herramientas, plataformas y enfoques que podrían mejorar sus estrategias de comunicación y mantenerlas competitivas, siendo un conocimiento necesario para la inteligencia táctica.

Desafíos para la inteligencia táctica

De acuerdo con la información recopilada en el presente estudio, la inteligencia táctica oportuna y relevante permite identificar amenazas emergentes y tomar medidas preventivas antes de que se conviertan en desafíos mayores o amenazas contra la seguridad y defensa nacional. Asimismo, facilita la coordinación entre las diferentes agencias y actores involucrados en la seguridad nacional, dado que proporciona una visión común de la situación y las prioridades. A pesar de lo antes señalado, es importante destacar que existen desafíos, tales como:

Comandos con demostrada experiencia en la especialidad: Es necesario que los directivos en las instituciones donde se produce inteligencia táctica o estratégica sean profesionales especializados en la materia, actualizados en las normas que la regulan y derechos humanos, considerando que el personal de inteligencia espera de sus líderes: orden, objetivos claros y confianza.

Recursos humanos eficientes: La producción de inteligencia táctica y estratégica requiere de personal capacitado y especializado -además de su profesión- en nuevas plataformas y lenguajes de comunicación que incluye a la inteligencia artificial, redes sociales y metalenguaje, herramientas y técnicas analíticas para la producción de inteligencia, así como la gestión de grandes volúmenes de datos (*big data*).

Plataformas integradas: Que comprenda la unidad de criterio para el almacenaje (fichas) de la información e inteligencia básica, actual y predictiva; ello contribuye a la coordinación efectiva entre las agencias de inteligencia.

Inversión en tecnología: La rápida evolución de las tecnologías de la información y la comunicación, incluida la inteligencia artificial, presentan desafíos y oportunidades en la producción de inteligencia táctica y estratégica.

Articulación interinstitucional: La limitada articulación, coordinación y colaboración entre componentes representa potenciales consecuencias en la duplicación de esfuerzos, superposición de funciones y falta de sinergia.

En este contexto, surge la necesidad de mejorar la capacidad de inteligencia táctica, principalmente, para anticipar y responder eficazmente a los desafíos de seguridad y las transformaciones geopolíticas y geoestratégicas que contribuyen a la producción de inteligencia estratégica nacional.

Conclusiones

La importancia de la inteligencia táctica, militar y policial, en la producción de inteligencia estratégica nacional radica en la estrecha interconexión entre ambas. Para lo cual, se destaca la capacidad de la inteligencia táctica para suministrar los detalles transcendentales que enriquecen la formulación de inteligencia estratégica a un nivel más amplio, dado que proporciona información detallada y contextual sobre eventos y actividades en curso. Por ello, se puede afirmar que la inteligencia táctica se convertiría en la herramienta sobre la cual se toman las decisiones en el más alto nivel gubernamental.

Por otra parte, se identificaron limitaciones en la producción de inteligencia táctica que deben abordarse, como la necesidad de mejorar la coordinación y colaboración entre las agencias de inteligencia, la capacitación y el desarrollo de habilidades de los analistas, así como el uso efectivo de las tecnologías de la información y la comunicación. Asimismo, se sugiere que se realicen investigaciones futuras para profundizar en el análisis de casos específicos y evaluar el impacto de la producción de inteligencia táctica en la toma de decisiones estratégicas en diferentes contextos.

El incremento exponencial en el flujo de la comunicación a través de las redes sociales ha generado extensos volúmenes de información en tiempo real, ofreciendo una fuente inigualable de datos para la inteligencia. A su vez, el uso masivo de la inteligencia artificial (IA) ha transformado la capacidad de análisis, permitiendo la identificación de patrones y correlaciones en grandes conjuntos de datos de manera más rápida y precisa. La aplicación de herramientas de big data ha permitido la extracción de conocimientos profundos a partir de conjuntos masivos de información, lo que ha redefinido la forma en que se abordan y comprenden los desafíos de seguridad, así como el proceso de toma de decisiones estratégicas.

En síntesis, la producción de inteligencia táctica es fundamental para la generación de inteligencia estratégica, puesto que un país que invierte en la mejora de su capacidad de producción de inteligencia táctica estará en una posición ventajosa para enfrentar los desafíos y aprovechar las oportunidades en el escenario geopolítico actual. La comprensión de esta relación y la aplicación efectiva de la producción de inteligencia táctica son esenciales para la seguridad nacional y el bienestar general.

Referencias

Agencia Central de Inteligencia de Estados Unidos. (1981, 04 de diciembre). Una estimación crucial revivida, por Sherman Kent. https://www.cia.gov/readingroom/docs/CIADP80M01009A000300420003- 8.pdf

Bogran, J., Lazo, W., y Zometa, D. (2015). El impacto de la Inteligencia Policial en la toma de decisiones estratégicas, operativas y tácticas en la Policía Nacional Civilde El Salvador. Revista Policía y Seguridad Pública, 2(5), 351-414. https://doi.org/10.5377/rpsp.v5i2.2330

Cabrera, L. (2016). La inteligencia estratégica: una herramienta necesaria para la toma de decisiones en el Estado del siglo XXI. Revista Policía y Seguridad Pública, 5(2),183-208. https://doi.org/10.5377/rpsp.v5i2.2329

De Miguel, J. (2021). La inteligencia estratégica aplicada al cambio. Iuris Tantum, 35(34), 57-71. https://doi.org/10.36105/iut.2021n34.03

Fuld, L. (1995). The New Competitor Intelligence. The Complete Resource for Finding, Analyzing and Using Information About Your Competitors. Wiley.

Gearon, L. (2015). Education, security and intelligence studies. British Journal of Educational Studies, 63(3), 263-279. https://www.jstor.org/stable/43896287

Hulnick, A. (2006). What's wrong with the Intelligence Cycle? Intelligence and National Security, 21(6), 959-979. https://www.jstor.org/stable/j.ctt183q0qt

Kent, S. (1966). Strategic Intelligence for American World Policy. Prensa de la Universidad de Princeton. https://doi.org/978-1-4008-7915-1

Ministerio de Defensa de España. (2003). Revisión Estratégica de la Defensa. Ministerio de Defensa de España. https://www.defensa.gob.es/Galerias/defensadocs/revisionestrategica.pdf

Munar, L. (2010, 11 de junio). Inteligencia Táctica. Infodefensa.com.

Ordoñez, M., y Cruz, G. (2017). La inteligencia militar ecuatoriana en la sociedad del riesgo. URVIO. Revista Latinoamericana de Estudios de Seguridad, 21, 56-59. https://doi.org/10.17141/urvio.21.2017.2964

Saavedra, B. (2016). Inteligencia Estratégica en un mundo globalizado en Latinoamérica:Retos y desafíos en el siglo XXI. Revista Policía y Seguridad Pública, 5(2), 75- 105. https://doi.org/10.5377/rpsp.v5i2.2326

Sainz de la Peña, J. (2012). Inteligencia táctica. Revista UNISCI, 28, 213-232. https://www.redalyc.org/articulo.oa?id=76724473010

Tzu, S. (2021). El arte de la guerra completo. Penguin Random House Grupo Editorial.

Zuñiga, L. (2014). Metodología de la Investigación: Diferencias entre la Inteligencianacional y la inteligencia policial [Sesión de Conferencia]. Dirección de Inteligencia de la PNP, Lima, Perú.

Responsabilidad parental en la comisión del delito de pornografía infantil

Vanessa Málaga Ángeles

Escuela de Posgrado de la Policía Nacional del Perú

Introducción

El control parental es definido como el conjunto de mecanismos que ayuda a restringir, inspeccionar y acceder a las plataformas virtuales que emplean los menores de edad (Fernández, 2023), esto permite dar seguimiento a la información que no es apta para ellos.

La Convención sobre los Derechos del Niño (2000) manifiesta que «toda representación, por cualquier medio, de un niño dedicado a actividades sexuales explícitas, reales o simuladas, o toda representación de las partes genitales de un niño con fines primordialmente sexuales»" (párr. 2), vulnera los derechos fundamentales de los menores de edad, incluyendo a las que se expenden a través de las tecnologías de la información y comunicaciones.

En el Perú, la Policía Nacional del Perú (PNP), por mandato del Estado, asume la función de prevenir e investigar el delito (Constitución Política del Perú, 1993), proteger la vida y la seguridad de las personas, ya que se encuentra al servicio de la sociedad, dentro de sus primordiales funciones reconocidas en el ordenamiento nacional y están relacionadas al Orden Interno, el Orden Público, así como a la prevención e investigación del delito. Por consiguiente, persigue la comisión de delitos cometidos en cualquier contexto, incluidas aquellas que se realizan mediante el uso de las tecnologías de información o de comunicación que contengan material pornográfico de menores de edad (Ley de Delitos Informáticos Ley Nº 30096).

En ese contexto, el Decreto Supremo N.° 026-2017-IN del Reglamento del Decreto Legislativo N° 1267 Ley de la Policía Nacional del Perú (2017) establece que la División de Investigación de Delitos de Alta Tecnología de la PNP es responsable de la prevención, investigación y denuncia de los delitos informáticos cometidos a través de las tecnologías de la información y comunicación, encontrándose dentro de sus funciones la comisión del delito contra la indemnidad sexual de menores de edad en la modalidad de pornografía infantil y propuestas sexuales mediante los medios tecnológicos. Estos delitos se encuentran tipificados en el Código Penal (2016) en los artículos 183-A. Pornografía infantil y artículos 183-B. Proposiciones sexuales a niños, niñas y adolescentes, con penas privativas de libertad que van desde los seis a doce años.

Según Torrecillas et al. (2020), los padres de familia permiten que desde una temprana edad sus hijos utilicen sus dispositivos electrónicos sin un tiempo determinado, en un inicio verifican el contenido que visualizan; sin embargo, este control se va perdiendo conforme el menor va creciendo, en razón de que los dispositivos ya son de uso personal del menor y el control de los contenidos, así como la limitación de su uso son casi inexistentes o más difíciles de realizar, sin tener presente que la intervención que ellos puedan tener sobre sus hijos, sin interesar la edad que tengan, será más sólida a través del diálogo y consejos, basados en el desarrollo de las capacidades personales y sociales.

La pornografía infantil es un delito complejo que no puede ser evitado a causa del crecimiento de las tecnologías que se encuentran inmersas en nuestro día a día. Esto también implica una variedad de problemas sociales y psicológicos que originan la comercialización de prácticas antisociales mediante las plataformas digitales; es por ello que para un mejor conocimiento y manejo del Internet, las autoridades de Colombia han puesto en ejecución diversos programas que permiten al menor la utilización de las redes sociales y plataformas de internet (Noguera et al., 2022).

El abuso sexual infantil tiene una gran variedad de modalidades que proliferan mediante la utilización de las tecnologías de la información y la comunicación. De acuerdo a la División de Delitos de Alta Tecnología de la Policía Nacional, cada vez son más los menores de edad que tienen acceso a contenido pornográfico, esto a raíz de la facilidad de acceso a los dispositivos móviles. Asimismo, la sociedad civil reportó un aumento de contenido sexual de menores en páginas web nacionales (Acción por los niños, 2020).

Los padres son quienes permiten la sobreexposición de sus menores hijos al entorno digital, comprometiendo su integridad física y psicológica por personas mayores o al acceso a información inapropiada; transgrediendo las responsabilidades que el Estado delega a través de la autoridad parental (Suárez, 2022). Por lo tanto, se corre el riesgo de que en el metaverso un abusador puede acercarse a los niños, niñas o adolescentes de forma más rápida y eficaz que el mundo real, esto se debe a que las redes sociales le permiten recabar toda la información necesaria del entorno de la víctima y a través de las mismas, contactarla e interactuar para lograr sus fines delictuosos (Cruz, 2021).

Las tecnologías de la información y la comunicación (TIC) no solo han traído grandes beneficios en la población, sino que también se han desarrollado alarmas de violencia en el espacio virtual, esto ha traído consigo ciertas conductas agresivas que son el reflejo de su entorno familiar, su cultura y el sistema socioeconómico en el que se desenvuelven (López–Castro et al., 2021).

El internet ha permitido que los delincuentes recurran a la pornografía infantil, utilizando diferentes

fachadas para realizar sus actividades delincuenciales, por ello es importante que los padres, tutores y docentes lleven un control sobre los niños al momento de que hagan uso del internet y redes sociales, a fin de evitar que sean víctimas del delito de pornografía infantil (Cruz, 2019).

Cada vez se encuentran más expuestos en las redes sociales los menores de edad, al momento en el que realizan una publicación de sus datos personales o comparten fotografías personales, esto permite que personas inescrupulosas utilicen esa información para conocer todo de ellos. Por esa razón es necesario que las plataformas web implanten medidas de seguridad y que los padres de familia ejerzan un mayor control parental (Duran, 2022).

Según Zambrano y Dueñas (2019), la globalización y el avance de las tecnologías han ocasionado que el delito de pornografía infantil sea un problema internacional, esto ha permitido que sea catalogado por la sociedad como uno de los delitos más abominables, generando un rechazo a aquellos que se encuentren inmiscuidos en él, por lo que la sociedad ve que es necesario establecer medidas de protección hacia los niños y no sean víctimas de este delito.

Uno de los problemas más significativos que existen en la actualidad es la pornografía infantil; desafortunadamente, en el campo de la prevención es en el que menor cantidad de trabajo se ha realizado y, al ser un asunto amplio en el que intervienen varios factores, es pertinente plantear estrategias prácticas y efectivas que contribuyan a la prevención de este delito, por lo que tiene que ser abordado por el Estado (Colmenares et al., 2021).

Es importante que el Estado brinde protección a los niños, niñas y adolescentes, con regulaciones en el entorno digital que vayan acorde a sus derechos y autonomía, referente al acceso, formación y protección, donde deben de estar inmersos los padres, la familia, así como las instituciones educativas, con la finalidad de salvaguardar su integridad y supervisar el uso adecuado que sus menores hijos les dan a los dispositivos electrónicos, por ser el medio de captación usado (Suárez 2022).

En este contexto, el objetivo del presente artículo busca analizar la responsabilidad parental en la comisión del delito de pornografía infantil. Para ese fin, se describe de qué manera el control que los padres de familia ejercen sobre sus menores hijos como medida preventiva permitirá disminuir el delito de pornografía infantil, a través del monitoreo de navegación y de la restricción de contenidos a los que sus hijos tienen acceso.

Método

La presente investigación busca producir conocimiento a partir del análisis de la realidad, por lo que estamos frente a una investigación básica o pura, el enfoque fue cualitativo, por lo que procedió a recolectar y analizar la información procedente de las experiencias de las personas involucradas en el fenómeno de estudio (Hernández et al., 2014).

El diseño de la investigación fue fenomenológico. La fenomenología es una manera de acceder a lo que los humanos encuentran en el día a día, es parte fundamental del mundo que habitamos, en otras palabras, a los fenómenos con el objetivo de descubrir la estructura y significado de estos fenómenos (Gonzáles, 2023). Asimismo, se utilizó el método inductivo para obtener conocimiento a partir de la realidad específica, así como de las rutinas y conocimientos de los mecanismos de seguridad en menores hijos (Dávila, 2006).

Para el presente artículo, se utilizó la entrevista y la revisión de las normas legales relacionadas a la Ley de Delitos Informáticos, Código Penal, Ley del Código de los Niños y Adolescentes, así como la Ley de la PNP en base a la responsabilidad parental y la protección de los menores de edad en el entorno digital, contenidos en las leyes y reglamentos. Asimismo, se procedió a entrevistar a doce (12) padres de familia que cuentan con formación universitaria, con hijos que se encuentran cursando educación primaria y secundaria.

Respecto a los instrumentos utilizados, para las entrevistas se utilizaron las guías de entrevista sobre la responsabilidad parental y protección del menor en el entorno digital.

Para la recopilación de datos cualitativos, se procedió a realizar el procedimiento conforme a la técnica seleccionada; para ello, en la entrevista, se contactó a los participantes; consecutivamente, se les informó acerca de la investigación y se les solicitó el consentimiento informado, de modo que la investigación se rija por los principios éticos. Por último, se entrevistó a los especialistas contactados y se grabó la información.

En el procesamiento de datos, se transcribió la información obtenida en las entrevistas, Luego, a través de la técnica de análisis de contenido, se partió la información obtenida de las respuestas. Se contrastó la información adquirida con las subcategorías o las categorías predeterminadas, más adelante se sintetizó.

Resultados

De acuerdo a las familias 4 y 7, se mencionó que los hijos utilizaban principalmente el celular, la tablet y la computadora, donde el uso del celular es para la comunicación, la tablet para el entretenimiento, y la computadora era usada para tareas escolares e investigaciones (Familia 1, 2 y 3). Se observó que el uso de estos dispositivos comenzaba desde temprana edad, alrededor de los 4 años para la tablet (Familia 9), 8 años para el celular (Familia 12) y a partir de los 12 o 13 años para la computadora (Familia 6, 7, 8).

Los entrevistados comentaron que el crecimiento de los hijos conlleva un proceso natural de desarrollo que impacta en su relación con la tecnología y, por ende, en la dinámica del control parental. A medida que los hijos maduran, adquieren mayor independencia en el manejo de dispositivos electrónicos, lo que representa un desafío en términos de supervisión y orientación (Familia 10). Refiriendo a las familias 8 y 11, la presencia de conflictos al tratar de establecer límites y la necesidad de los adolescentes por sentir que tienen mayor control sobre sus vidas.

Esta evolución hacia la independencia dificulta el control parental sobre las actividades de los hijos. Los padres, conscientes de esta realidad, tienden a depender en gran medida de la supervisión directa como principal método para monitorear el contenido al que acceden sus hijos en Internet (Familia 12). Sin embargo, esta estrategia se vuelve menos efectiva, ya que los jóvenes pueden encontrar formas de eludir o evadir la supervisión (Familia 2).

Por otra parte, se observa que algunos padres reconocen la importancia de utilizar herramientas de protección, como filtros de contenido y controles parentales, estas soluciones son mencionadas en menor medida (Familia 4). Por lo que se relaciona con la falta de familiaridad de los padres con estas herramientas (Familia 2-6) o con la percepción errónea de que la supervisión directa es suficiente para proteger a sus hijos en línea (Familia 1, 9, 10).

Esto permitió que se reconociera que existe una falta de comprensión tecnológica por parte de los padres que puede dejar a los niños vulnerables a los peligros en línea, incluida la exposición a la pornografía infantil (Familia 1, 2, 3, 4). También se reconoció la ausencia de entendimiento, que conlleva una negligencia involuntaria por parte de las familias en cuanto a la protección de sus hijos de contenidos inapropiados en Internet.

Además, la confianza que los padres depositan en sus hijos al utilizar dispositivos electrónicos, es aceptada por consenso de que no es suficiente para prevenir la comisión de delitos en línea. Aunque es importante, no sustituye la necesidad de una supervisión activa y una comunicación franca sobre los riesgos asociados con el uso de Internet. Expresan algunos padres que no solo depende de la confianza, sino también de establecer límites claros y normas de comportamiento en línea (Familia 8, 12).

Los resultados resaltan la importancia de establecer medidas de protección en el entorno digital para garantizar la seguridad de los menores hijos, ello incluye la supervisión de la cantidad de información que

publican en sus redes sociales y el desarrollo y fortalecimiento de los vínculos afectivos entre padres e hijos, permitiendo que las situaciones relacionadas a la pornografía infantil sean detectadas a tiempo, aún antes de que el menor de edad haya enviado, publicado o mostrado ante una cámara web una parte del cuerpo desnuda.

Aceptando las familias que, si bien, los dispositivos electrónicos pueden ser herramientas útiles para el aprendizaje y la comunicación, también representan riesgos, como ser engañados por criminales que los incitan a realizar fotos o videos en situaciones comprometedoras o el acceso a contenido inapropiado, que distorsionan la apreciación de la sexualidad en un menor.

Discusión

Los resultados de la investigación resaltaron los desafíos que enfrentan los padres para supervisar las actividades en línea de los hijos a medida que estos crecen. La naturaleza inherente del deseo de independencia puede entorpecer la comunicación abierta entre padres e hijos, lo que puede llevar a que los jóvenes actúen con mayor cautela y eviten compartir detalles sobre sus experiencias en línea. Esta falta de comunicación puede limitar la capacidad de los padres para identificar posibles incidentes o problemas relacionados con la exposición a la pornografía infantil u otros peligros.

Torrecillas et al. (2020), identifica una situación similar, refiriendo que, aunque el vínculo inicial entre los padres-hijos puede ser fuerte, el control que se establece sobre posibles conductas de riesgo, va reduciéndose con el tiempo. Por su parte, Cruz (2021) señaló que el metaverso permite a los abusadores acceder con facilidad a la información personal que publican los menores de edad en sus redes sociales, posibilitando un acercamiento más dinámico y efectivo al que se tiene en el mundo real, aunado al poco control, convirtiendo al menor de edad en un objetivo fácil. De igual forma, Cruz (2019), indica que los delincuentes recurren a la pornografía infantil mediante el uso de Internet y redes sociales como canales de captación.

Por otra parte, padres de familia han señalado que la supervisión directa es la mejor solución ante esta situación, limitando su espectro de acción al mismo; hecho que puede complementarse con otros programas de protección y filtros que limitan la interacción de los menores de edad cuando se encuentran en línea. Este hallazgo es coherente con la propuesta de Suárez (2022), quien destaca la responsabilidad de los padres para proteger la integridad física y psicológica de sus menores hijos al sobreexponerlos a la interacción digital, sin tener presente el control parental que deben ejercer en ellos. No obstante, Noguera et al. (2022) señalaron que el delito de pornografía infantil se configura como un fenómeno complejo, que difícilmente puede ser evadido, considerando el incesante crecimiento de las tecnologías, así como las prácticas antisociales a través de las plataformas digitales.

Fernández (2023) señala que el control parental ayuda a restringir, inspeccionar y acceder a las plataformas virtuales que emplean los menores de edad. Asimismo, Duran (2022), resalta que es necesario que las plataformas web establezcan medidas de seguridad para que los padres de familia practiquen un correcto control parental sobre sus hijos menores de edad. Al respecto, Suárez (2022) resalta lo relevante que es la participación del Estado en la protección de los menores de edad en el entorno digital y el trabajo conjunto que se debe realizar con la familia e instituciones educativas, para salvaguardar la integridad del menor.

Conclusiones

Tras analizar los resultados de la investigación, se puede concluir que la pornografía infantil es un delito complejo que no puede ser evitado por la evolución de las tecnologías y las buenas prácticas que se dan mediante las plataformas digitales. En este sentido, es fundamental que las autoridades peruanas establezcan programas que brinden un uso seguro del Internet dirigido a menores de edad, así como implantar medidas de seguridad para que los padres ejerzan un adecuado control parental sobre sus hijos

cuando estos utilicen las plataformas web.

Los resultados también revelaron que el uso de dispositivos electrónicos por parte de los hijos comienza desde temprana edad, lo que dificulta el control parental a medida que los hijos crecen. Por lo tanto, es crucial que los padres tomen conciencia sobre la responsabilidad parental como prevención del delito de pornografía infantil, estableciendo límites y supervisando el adecuado uso de todos los dispositivos electrónicos que los menores manipulan, sobre todo cuando son más pequeños, por no tener la capacidad de comprender el contenido al que acceden.

En conclusión, la responsabilidad parental juega un papel crucial en la prevención del delito de pornografía infantil en el Perú y es necesario implementar programas de educación, establecer medidas de protección en el entorno digital y promover la supervisión activa por parte de los padres para garantizar la seguridad de los menores hijos.

Referencias

Acción por los niños (2020). Mapeo de acciones implementadas por las empresas de tecnologías de la información y comunicación (TIC) para la protección de la niñez y la adolescencia contra la violencia sexual en línea. Paz y Esperanza. https://accionporlosninos.org.pe/pdf/Recomedaciones-TICs.pdf

Colmenares, L., León, M. y Cerón, C. (2021) Perspectiva de los universitarios sobre la pornografía infantil y propuesta de prevención. Indoamérica, 10(01), 1-13. http://portal.amelica.org/ameli/jatsRepo/367/3672094006/index.html

Cruz, A. (2019). Delito de pornografía infantil una realidad escolar y comunitaria. Revista Arbitrada Interdisciplinaria Koinonía, 4(8), 722. https://doi.org/10.35381/r.k.v4i8.396

Cruz, L. (2022). El "Child Grooming" y regulación del delito sexual virtual contra niños, niñas y adolescentes en Colombia. Derecho Penal y Criminología, 42(113), 43-96. https://doi.org/10.18601/01210483.v42n113.03

Dávila, G. (2006). El razonamiento inductivo y deductivo dentro del proceso investigativo en ciencias experimentales y sociales. Laurus, 12, 180-205. https://www.redalyc.org/comocitar.oa?id=76109911

Decreto Legislativo N°635, Código Penal del Perú (2024). Diario el Peruano. https://lpderecho.pe/codigo-penal-peruano-actualizado/

Decreto Supremo N° 026-2017-IN del Reglamento del Decreto Legislativo N°1267 Ley de La Policía Nacional Del Perú (2017). Diario oficial el peruano. https://elperuano.pe/normaselperuano/2017/10/15/1576324-1/1576324-1.htm.

Duran, S. (2022) Menores en internet: problemas del ejercicio de la patria potestad sobre los "nativos digitales". Revista Actualidad Jurídica Iberoamericana, 17(2). https://dialnet.unirioja.es/servlet/articulo?codigo=8737291

Fernández, N. (2023). Intervention on parental control. Revista Internacional Interdisciplinar De Divulgación Científica, 1(1). https://riidici.com/index.php/home/article/view/9.

González, L. (2023). El ser del hombre a la luz del Popol Vuh. Análisis fenomenológicohermenéutico. LiminaR. Estudios sociales y humanísticos 21(1) 45. https://doi.org/10.29043/liminar.v21i1.948.

Hernández, R., Fernández, C., y Baptista, P. (2014). Metodología de la investigación (6ta edición). Mac Graw Hill.

La Convención sobre los Derechos del Niño (2000). Explotación de niños, niñas y adolescentes en Internet. http://www.iin.oea.org/boletines/especial21/4-esp.html.

Ley N°30096, Ley de Delitos Informáticos (2013). Ministerio Público Fiscalía de la Nación https://www.gob.pe/institucion/mpfn/informes-publicaciones/1678028-ley-n-30096

López-Castro, L., López-Ratón, M., y Priegue-Caamaño, D. (2021). Tipos de mediación parental del uso de las TIC y su relación con la cibervictimización del alumnado de educación primaria. Bordón: Revista de pedagogía, 73(2), 97-111. https://dialnet.unirioja.es/servlet/articulo?codigo=8015451

Noguera, M., Edotti, L., Galofre, A., Martínez, A., Martínez, L., y Guzmán, P. (2022). La pornografía infantil en entornos digitales en Colombia. Revista Virtual Tejidos Sociales, 5(2). https://revistas.unisimon.edu.co/index.php/tejsociales/issue/view/280

Presidencia de la República del Perú. (1993). Constitución Política del Perú. Congreso de la República. https://www.gob.pe/institucion/presidencia/informespublicaciones/196158-constitucion-politica-del-peru

Suárez, L. (2022). La responsabilidad parental en los entornos digitales. Necesario equilibrio entre acceso, control y seguridad. Actualidad jurídica iberoamericana, 1(17), 1076- 1097. https://dialnet.unirioja.es/servlet/articulo?codigo=8737287

Torrecillas, T., Vázquez, T., Suárez, R., y Fernández, L. (2020). El papel de los padres en el comportamiento online de menores hiperconectados. Revista Latina, 1(75), 121-148. https://doi.org/10.4185/RLCS-2020-1419

Zambrano-Mendieta, J., y Dueñas-Zambrano,K.(2019). Un acercamiento al abuso sexual infantil. La pornografía. Polo del Conocimiento: Revista científico - profesional, 4(6), 192-207. https://dialnet.unirioja.es/servlet/articulo?codigo=7164358

Problemática en el procedimiento para el levantamiento de cadáveres

Carlos Guerrero Matta

Ronald Elmer Salas Calizaya

Richar Cristian Becker Loaiza

Escuela de Posgrado de la Policía Nacional del Perú

Introducción

Tras una exhaustiva revisión de manuales y protocolos emitidos por diversos institutos relacionados con la criminalística y ciencias forenses, así como la normativa que regula el modelo procesal penal, se han constatado coincidencias en la secuencia de actividades que se realizan en el lugar donde se ha producido un hecho criminal con subsecuente muerte. Sin embargo, al abordar específicamente la diligencia de levantamiento de cadáveres, se evidencia una variabilidad en los actores involucrados y en el seguimiento riguroso de la secuencia protocolar. En algunos casos, el traslado del cadáver no se ejecuta siguiendo estándares técnicos o profesionales, descuidando aspectos críticos como la bioseguridad y los procedimientos para el tratamiento del cadáver. Esta falta de apego a los protocolos expone al cadáver a riesgos ambientales y potenciales contagios, revelando la importancia de investigar el rol del principal encargado de analizar la escena del crimen, así como ciertos elementos específicos de la misma, un interés que varios autores han destacado, especialmente en el contexto actual.

En relación a este tema, Palomo et al. (2004) plantea la persistente incógnita sobre quién debe asumir el papel principal en el análisis de las circunstancias y elementos presentes en la escena del crimen, particularmente cuando se trata de casos que implican fallecimientos. Por su parte, Nogué-Navarro et al. (2016) señalan que, desde tiempos remotos, las sociedades han mostrado interés en el estudio de los cuerpos humanos cuando estos sufren lesiones durante conflictos bélicos o son objeto de rituales sacrificiales. En este contexto, Finkbeiner et al. (2009) menciona el ejemplo del antiguo Egipto, donde el historiador Manetón relata que el faraón médico Athotis escribió tratados de medicina que incluían descripciones anatómicas alrededor del año 4000 antes de Cristo (a.c.).

Determinar la defunción de un individuo reviste gran importancia para llevar a cabo el protocolo de levantamiento del cadáver. En este sentido, Pérez (2016) indica que, desde una perspectiva médica, la muerte implica la extinción de todas las funciones biológicas del organismo, manifestándose a través de un proceso gradual de descomposición celular que culmina en la muerte biológica. Desde la práctica clínica, el diagnóstico de la muerte se basa en el cese de las funciones cardíacas, respiratorias y neurológicas, mientras que, desde el ámbito jurídico, se establece la pérdida de la personalidad jurídica una vez que se ha certificado la muerte biológica.

Por consecuencia, el levantamiento del cadáver alude al proceso que se inicia con la llegada del médico forense a la escena del crimen para certificar la hora aproximada del fallecimiento, describir el estado del cadáver y las lesiones presentes, así como proceder al recojo, traslado e internamiento en el Instituto de Medicina Legal o entidad equivalente, donde se llevará a cabo la correspondiente necropsia (Robledo et al., 2013). Este procedimiento legal implica la inspección del cuerpo sin vida en el lugar donde ocurrieron los acontecimientos, siendo fundamental la presencia del médico forense. Esta actividad es realizada por una comisión judicial, en colaboración con expertos forenses y la autoridad policial encargada de las investigaciones.

En el contexto mencionado, tanto manuales como protocolos, así como la normativa del modelo procesal penal, coinciden en que las primeras diligencias preliminares de investigación realizadas en la escena de un crimen con muerte sospechosa o de criminalidad requieren una formación básica en conocimientos criminalísticos. Estos conocimientos son esenciales para llevar a cabo la diligencia de aislamiento y protección de la escena del crimen. El personal policial, en su calidad de primer interventor, debe delimitar y describir en un acta u otro documento el espacio que debe asegurar para preservar la integridad del cadáver, así como los indicios, vestigios y evidencias presentes en el lugar del crimen.

Fernández et al. (2020) destacan que la inspección del lugar donde se presume que se ha cometido un delito es una actividad investigativa crucial en el ámbito de la justicia penal, ya que el éxito de esta diligencia determina el curso de la etapa de investigación o instrucción. Del mismo modo, Pachar (2018) comenta que el análisis científico de la escena del crimen desempeña un papel fundamental en las investigaciones judiciales. Un equipo multidisciplinario, que incluye al médico forense como parte esencial, lleva a cabo esta tarea. Conocer las circunstancias y antecedentes del incidente bajo investigación, así como estudiar tanto el lugar de los hechos como el cuerpo sin vida, son elementos indispensables para abordar adecuadamente la autopsia. El objetivo principal del trabajo pericial médico forense es contribuir a esclarecer la comisión de un delito con resultado de muerte.

Siguiendo con el procedimiento, con la llegada de los peritos se desarrolla la diligencia criminalística especializada, que inicia con la recepción de la escena del crimen, procediendo a ingresar para perennizar la escena, así como el respectivo recojo de los indicios, evidencias y vestigios que se encuentren, pudiendo determinarse en dicho acto con conocimiento del representante del Ministerio Público en otros casos del Juez Instructor, el ingreso del Médico Legista, para que ingrese a la escena del crimen y proceda con la diligencia de levantamiento del cadáver, que de conformidad con la doctrina desarrollada por medicina legal, esta inicia cuando el médico legista inspecciona el cadáver y hace una descripción de la posición, lesiones externas visibles entre otras necesarias que contribuyan al esclarecimiento del hecho las mismas que serán corroboradas posteriormente con la necropsia de ley.

Fernández et al. (2020) enfatizan que para llevar a cabo la inspección del lugar donde ocurrió el evento, es esencial que los participantes cuenten con una formación completa en criminalística, lo que les permitirá recopilar la mayor cantidad de información posible relacionada con un acto delictivo relevante. Siempre existe la posibilidad de obtener evidencias o rastros que ayuden a determinar cómo y quién pudo haber llevado a cabo dicho acto, como lo establece el conocido principio de intercambio en el ámbito criminalístico, donde cuando una persona abandona un lugar, siempre se lleva algo consigo y, a su vez, deja algo que le pertenece.

Considerando que la criminalística y la medicina forense son disciplinas que proporcionan conocimientos generales y específicos según cada caso, se esperaría que el procedimiento y los profesionales que realizan la diligencia de levantamiento de cadáver siguieran un estándar común. Sin embargo, como se ha observado, existen marcadas diferencias en los procedimientos llevados a cabo por los operadores de justicia y los profesionales forenses en diferentes países. Esto se refleja en la diversidad de actores involucrados en la realización de esta labor. Por ejemplo, en algunos casos, la diligencia de levantamiento de cadáver es realizada por médicos forenses, en otros por personal policial, y en otros por un policía que actúa como primer interviniente, pesquisa o perito criminalístico. En algunos casos, esta diligencia es realizada por representantes del Ministerio Público, mientras que en otros participan todos ellos como un equipo multidisciplinario.

En relación a esto, Fernández et al. (2020) han destacado que, siguiendo los principios de la criminalística, examinar la escena del crimen o el lugar donde se presume que ocurrió un acto ilegal es importante para formular hipótesis que generen sospechas e inicien el proceso de investigación. El objetivo principal de este proceso es determinar lo que sucedió, identificar al posible responsable y tomar decisiones acordes a la ley que guíen el curso de la investigación. En este contexto, Nogué-Navarro et al. (2016) señalan que la autopsia, que implica el análisis de un cuerpo después de la muerte, comienza desde el levantamiento del cadáver e incluye una evaluación externa e interna. La evaluación externa implica una inspección minuciosa del cuerpo, recopilando todos los detalles que puedan proporcionar indicios relevantes sobre la identificación y la causa del fallecimiento.

En cuanto a los actores encargados de realizar la diligencia del levantamiento del cadáver, en Colombia, de acuerdo con el Artículo 214 de la Ley 906 “Código de Procedimiento Penal Colombiano”, la diligencia preliminar es llevada a cabo por personal policial (Policía Judicial). En esta fase, son los pesquisas y peritos de criminalística quienes abordan la escena del crimen y proceden a la inspección y levantamiento del cadáver, embalándolo técnicamente de acuerdo con los manuales de criminalística. Posteriormente, se traslada al centro médico legal con la orden de practicarse la necropsia, sin que en esta diligencia se cuente con la presencia física del médico legista o del representante del Ministerio Público.

En Chile, el levantamiento de cadáveres se lleva a cabo por la Policía en su papel de investigación primaria, según lo establecido en el artículo 90 del Código Procesal Chileno. Este artículo, publicado en el Diario Oficial el 12 de diciembre de 2000 y actualizado el 11 de julio de 2002, autoriza a la Policía (Policía de Investigaciones y Carabineros), con el conocimiento y la autorización del representante del Ministerio Público, a realizar el levantamiento de cadáveres encontrados en la vía pública, dejando constancia de la acción realizada. Aunque la normativa específica permite que la Policía lleve a cabo esta diligencia, en la práctica es el Servicio Médico Legal (SML) el organismo encargado de realizarla. Este organismo, que no está explícitamente mencionado en el modelo procesal penal chileno, lleva a cabo funciones criminalísticas y forenses, cuya competencia funcional se presume regulada por otra normativa.

En España, el procedimiento para el levantamiento de cadáveres sigue una vertiente diferente; de acuerdo con el artículo 28 del Código Procesal Penal, se establece la formación de un equipo multidisciplinario compuesto por unidades adscritas que brindan asistencia directa y prioritaria al Juzgado y Fiscal de guardia, así como a otros órganos del orden jurisdiccional. Este equipo realiza diligencias de investigación especializada, incluyendo inspecciones oculares, recolección de pruebas y el levantamiento técnico de cadáveres, entre otras actividades propias de una policía científica. Según Robledo et al. (2013),

este equipo se conoce como Comisión Judicial, y en caso de indicios evidentes de criminalidad, el Juez de Guardia, junto con el Secretario Judicial y el médico forense, participan en el levantamiento del cadáver. En ausencia de indicios evidentes de homicidio, el médico forense puede realizar la diligencia, aunque si surgen indicios después de su intervención, se notifica al Juez para convocar a la Comisión Judicial, que incluye al Juez, para llevar a cabo una investigación más exhaustiva.

A nivel internacional, se observan diversas modalidades para la realización del levantamiento de cadáveres en otros países. Aunque las diligencias previas al levantamiento del cadáver pueden coincidir, es probable que la ejecución varie significativamente. Con el fin de identificar problemas operativos y técnicos en esta diligencia y proponer soluciones, se analizará detalladamente un caso en Perú, donde la normativa que regula el proceso penal determina quién realiza esta diligencia. Esta situación conlleva la adopción de metodologías diferentes e incluso discrepancias en la ejecución, a pesar de existir conocimientos y técnicas forenses para el tratamiento adecuado del cadáver. Desde la inspección inicial del médico forense en la escena del crimen hasta el traslado e internamiento en el Instituto de Medicina Forense, donde se realiza la necropsia de ley, se observa un incumplimiento de los protocolos de bioseguridad y conservación del cuerpo como evidencia en cada etapa del proceso.

Conceptos y prácticas erróneas en la diligencia de levantamiento de cadáveres ocasionadas por el modelo procesal penal peruano

El modelo procesal penal peruano, promulgado mediante el Decreto Legislativo N° 957, conocido como el “Nuevo Código Procesal Penal”, establece en su artículo 195, numeral 2, que la diligencia de levantamiento de cadáveres es llevada a cabo por el fiscal, con la posible intervención del médico legista y del personal policial especializado en criminalística. Sin embargo, la participación de este último no es obligatoria según la normativa, dejando su implicación a la discreción del fiscal. En caso de delegación, la normativa jerarquiza la responsabilidad, permitiendo al fiscal adjunto ser el primer designado, seguido por el personal policial en caso de que el fiscal no pueda realizar la diligencia, y en última instancia, el juez de paz. Además, se contempla la posibilidad de que tanto el personal de las Fuerzas Armadas como de la Policía Nacional del Perú realicen esta diligencia en zonas declaradas en estado de emergencia, cuando el fiscal no pueda participar.

Es relevante destacar que, en el contexto peruano, existe una única fuerza policial que desempeña diversas funciones. Toscano (2020) identifica tres roles policiales en el ámbito de la investigación criminal: el primer interventor, generalmente a cargo del servicio de patrullaje y seguridad, encargado de llegar a la escena del crimen y asegurarla; la pesquisa, compuesta por personal especializado en investigación criminal; y el perito criminalístico o policía científica, responsable de la preservación y recolección de evidencia en la escena del crimen, empleando técnicas forenses para emitir peritajes. A pesar de esta distinción de roles establecida en las leyes y reglamentos que rigen a la Policía Nacional del Perú, el Ministerio Público no siempre reconoce esta diferenciación, lo que genera discrepancias entre los funcionarios encargados de la persecución del delito.

En el contexto normativo peruano, la responsabilidad de realizar la diligencia de levantamiento de cadáveres recae en el fiscal, quien tiene la facultad de delegar esta tarea a otros actores. Sin embargo, es importante resaltar que el único actor con formación técnica y científica forense adecuada para esta labor es el personal policial que cumple el rol de perito criminalístico. La normativa exige que antes de delegar esta función, el fiscal emita una disposición motivada que justifique la intervención de la Policía u otro actor, enfocando dicha delegación desde una perspectiva técnica y científica, y manteniendo los estándares de bioseguridad.

Resulta contradictorio que la normativa no incluya al médico forense como actor principal en la diligencia de levantamiento de cadáveres, siendo este profesional el más especializado y cuya participación es fundamental para obtener resultados precisos. La Fiscalía de la Nación del Ministerio Público (2007) ha reconocido esta necesidad en la Resolución de la Fiscalía de la Nación N° 129 -2007-MP-FN, que aprueba

el Manual de Procedimientos de la Diligencia de Levantamiento de Cadáver, donde se destaca el papel del médico legista y del equipo de profesionales en Ciencias Forenses en la investigación de la escena del crimen, cuyo objetivo es determinar las circunstancias de la muerte y la necesidad de una investigación más profunda.

Un caso ilustrativo de la problemática abordada en este artículo es el incidente relacionado con un individuo fallecido, a quien se referirá como Jesús, ocurrido en la ciudad de Arequipa. En este suceso, se evidenciaron omisiones en las diligencias previas al levantamiento del cadáver, como se detalla a continuación. Tras el fallecimiento de Jesús, los médicos del hospital inicialmente atribuyeron la causa de su muerte a causas naturales, pero posteriormente cambiaron su diagnóstico sin emitir el certificado de defunción correspondiente. Esta situación llevó a una comunicación, tanto verbal como escrita, con el Ministerio Público para coordinar el levantamiento y traslado del cuerpo a la morgue del Instituto de Medicina Legal de Arequipa. En estas comunicaciones se indicó que, de confirmarse causas no naturales de la muerte, se requeriría la intervención de la unidad especializada de investigación criminal, conocida como DIVINCRI, así como del personal policial especializado.

Sin embargo, el fiscal de turno optó por delegar la realización del levantamiento del cadáver al personal de la Comisaría Santa Marta, omitiendo las formalidades legales establecidas. Este hecho marcó el primer error en el procedimiento, generando discrepancias entre el personal policial y el Ministerio Público. Tras una serie de comunicaciones verbales y escritas, la DIVINCRI Arequipa concluyó que no era necesario intervenir al no identificar causas criminales. En contraste, el fiscal adjunto intentó delegar al personal policial el recojo, traslado e internamiento del cadáver, sin haberse presentado en el lugar ni coordinado con el médico forense, como lo exige la normativa. Estas infracciones a las normas y procedimientos por parte del Ministerio Público llevaron al personal policial de la Comisaría a rechazar la diligencia, argumentando que no era de su competencia y que no se habían seguido las formalidades legales. Esta situación provocó una reacción negativa por parte del fiscal titular, quien denunció administrativamente al personal policial por supuesta omisión del deber funcional al no cumplir con su orden. Sin embargo, la investigación subsiguiente determinó que el personal policial no había incurrido en ninguna infracción administrativa. Este resultado fue comunicado a los órganos de control del Ministerio Público para su evaluación y para la posible mejora de los procedimientos.

Finalmente, la diligencia de levantamiento del cadáver de Jesús fue llevada a cabo por personal policial especializado en criminalística, perteneciente a la OFICRI (Oficina de Criminalística), unidad técnica científica adscrita a la DIVINCRI (Dirección de Investigación Criminal). Este resultado se logró como parte de un acuerdo entre los responsables de ambas instituciones. Lamentablemente, hasta la fecha, el procedimiento no ha sido objeto de un debate adecuado y en la práctica se observa una diversidad de actores encargados de realizar el levantamiento de cadáveres en el Perú. En algunos casos, esta tarea recae en el personal policial en su papel de primer interviniente, mientras que en otros casos lo realiza el personal de investigación criminal o el personal especializado en criminalística. Siendo consistente en la mayoría de los casos la ausencia del representante del Ministerio Público y del médico forense, lo cual es preocupante. Es necesario resaltar la situación actual en el Perú, que posiblemente se refleje en otros países, a modo de demostrar la importancia de regular de manera adecuada y profesional las diligencias de levantamiento de cadáveres. La falta de una ejecución profesional de estas diligencias puede obstaculizar las investigaciones destinadas a determinar las responsabilidades en casos de homicidio, al no proporcionar una recolección de evidencia adecuada y exponerse a situaciones que podrían contaminar la escena del crimen o representar un riesgo de contagio por contacto directo con el cadáver. Además, es esencial señalar que los operadores encargados de la investigación podrían estar incurriendo en la comisión de un delito al no seguir los protocolos establecidos por la normativa que regula el modelo procesal penal, al no resolverse estas discrepancias competenciales.

Como resultado de la investigación administrativa contra el personal policial, se ha establecido claramente que el representante del Ministerio Público subdivide la diligencia de levantamiento de cadáver en tres etapas, cada una de las cuales requiere la participación de actores diferentes. En la primera etapa,

se lleva a cabo la observación y descripción del cadáver, que debe ser realizada por el médico legista para confirmar la muerte, determinar la hora y posibles causas. En la segunda etapa, el cadáver es recolectado y trasladado, tarea que debe realizarse con protocolos de bioseguridad y protección adecuados, preferiblemente por personal técnico forense. Finalmente, en la tercera etapa, el cadáver es internado en la morgue del instituto médico forense, donde un médico forense llevará a cabo la necropsia de ley y elaborará un informe forense que servirá como evidencia en investigaciones y juicios posteriores.

Conclusiones

La forma como se han establecido los procedimientos de levantamiento de cadáveres, tanto en Perú como en distintos países, pueden poner en riesgo la bioseguridad del personal policial, la integridad del cadáver, así como la escena del crimen. A pesar que las legislaciones establecen la importancia de la formación en criminalística para las primeras diligencias en la escena del crimen, hay marcadas variaciones en los actores involucrados. En ese sentido, los peritos desempeñan una labor importante en la recolección de indicios y el levantamiento del cadáver, que luego se complementa con la necropsia.

En el proceso de levantamiento de cadáveres, se identifican tres etapas con actores debidamente diferenciados. Se propone que el personal profesional y técnico forense del Instituto Médico Forense se encargue de todas las etapas para garantizar la estandarización y el cumplimiento de los protocolos de bioseguridad y fomentar la coherencia en los procedimientos.

Para lograr un efectivo procedimiento de levantamiento de cadáveres es importante mejorar las coordinaciones entre las instituciones involucradas, para ello se sugiere realizar modificaciones legales y profundizar en la doctrina forense que permita garantizar la aplicación de estándares y protocolos adecuados para el levantamiento de cadáveres. Esto contribuiría a mejorar la calidad de las investigaciones y la obtención de pruebas forenses sólidas.

Finalmente, es importante promover la estandarización en los procedimientos de levantamiento de cadáveres y establecer procedimientos y normas claras dentro del marco legal, asignando los recursos y presupuesto necesarios para su cumplimiento. Para ello, sería beneficioso evaluar si es apropiado subdividirla o considerarla como una sola diligencia, recurriendo a la doctrina forense.

Referencias

Fernández, P., Peña, J., y Huertas, O. (2020, 28 de mayo). La inspección del lugar del hecho y la valoración legal de la huella o evidencia. Revista Logos Ciencia & Tecnología,12(3), 115–127. https://doi.org/10.22335/rlct.v12i3.1253

Finkbeiner, W., Ursell, P., y Davis, R. (2009). Autopsy Pathology: A Manual and Atlas EBook. Saunders Elsevier. https://books.google.es/books?id=fJ_zQ8rC4tAC&printsec=frontcover&hl=es#v=onepage&q&f=false

Ley 19696, Código Procesal Penal actualizado el 23 mayo 2023. (2000). Biblioteca de Congreso Nacional de Chile BNC. https://www.bcn.cl/leychile/navegar?idNorma=176595

Ley 906, Código de Procedimiento Penal Colombiano. (2004). Función Pública: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=14787

Ministerio de Justicia (2004). Decreto Legislativo 957, Nuevo Código Procesal Peruano. Sistema peruano de información jurídica. Ministerio de Justicia. https://spij.minjus.gob.pe/spij-ext-web/detallenorma/H682694

Nogué-Navarro, L., Bardalet N., y Adserias, M. (2016). Técnicas de apertura del Cadáver. Medicina Legal de Costa Rica, 33(1), 3-14. https://www.scielo.sa.cr/scielo.php?pid=S1409- 00152016000100003&script=sci_abstract&tlng=es

Pachar, J. (2018). La participación del médico forense en la escena del crimen. Medicina Legal de Costa Rica, 35(1), 102-114. https://www.scielo.sa.cr/scielo.php?script=sci_arttext&pid=S1409-00152018000100102

Palomo, J., y Ramos, V. (2004). Papel del Médico Forense en la Inspección Ocular y Levantamiento del Cadáver: Propuesta de documento. (Recomendaciones, guías, normas o protocolos de actuación profesional). Cuadernos de Medicina Forense, 10(36), 41-57. https://pesquisa.bvsalud.org/portal/resource/pt/ibc-94612

Pérez, R. (2016). Fundamentos de la medicina forense. Editorial UOC.

Resolución de la Fiscalía de la Nación N° 129-2007-MP-FN (2007). Que aprueba el Manual de Procedimientos de la Diligencia de Levantamiento de Cadáver, y el Manual de Procedimientos Tanatológicos Forenses y Servicios Complementarios. https://www.mpfn.gob.pe/Docs/iml/files/guia23.pdf

Robledo, M., Páez, N., Viñuela, P., y Hormigos, L. (2013). La Guardia Civil en el levantamiento del cadáver. Gaceta Internacional de Ciencias Forenses, 8, 25-38. https://dialnet.unirioja.es/servlet/articulo?codigo=4369839

Toscano, Y. W. (2020). Actuación policial desde la jurisprudencia, evolución de la casuística a la jurisprudencia. En Y. W. Toscano, Actuación policial desde la jurisprudencia, evolución de la casuística a la jurisprudencia. A&C Ediciones Jurídicas S.A.C.

Licitud restrictiva acerca del control de identidad policial

José Enrique Enriquez Chipana

Escuela de Posgrado de la Policía Nacional del Perú

Introducción

La génesis de la figura jurídica del Control de identidad policial (CIP), se remonta a la implementación del novísimo estatuto proceso penal peruviano, Decreto Legislativo N° 957 (2004), tal nomen iuris taxativamente se ubica en el artículo 205, desde su origen no ha sido reglamentado, solamente se modificó en octubre de 2023, mediante el Decreto Legislativo N° 1574, respecto al procedimiento de ciudadanos extranjeros. El CIP es usual en la vida diaria, en las calles y avenidas los policías suelen hacer «operativos policiales por CIP» con fines de prevención e investigación delictual, empero, su aspecto esencial radica en que es la actuación policial [indicador] que más se ejecuta en el país.

El Anuario Estadístico de la Policía Nacional del Perú (2020, 2021, 2022) señala que en el 2020 se realizaron 99,768 operativos, en el 2021 se practicaron 99,524 operativos, y en el 2022 se ejecutaron 135,938 operativos, alcanzado un total de 335,230 operativos por CIP en todo el Perú entre los años 2020 y 2022.

Tabla 1

Operativos policiales por CIP 2020-2023.

Departamento	2020	2021	2022
Amazonas	1754 3	324	2,753
Ancash	3,902 1	3217 1	5,662
Apurímac	3,514	4747 4	,520
Arequipa	12,276 1	1079	10,930
Ayacucho	801 7	00 1	,558
Cajamarca 6	,951 6	521	12,009
Callao	1,290	1386 1	,266
Cusco 1	,482 1	851	3,495
Huancavelica 2	94	331 9	32
Huánuco 6	,723	3403 4	,591
Ica 3	,589 1	675	1,292
Junín 2	73	3085	3,410
La Libertad	5,445 5	393	8,120
Lambayeque 6	,358 4	124	5,057
Lima	25,230 2	1436 2	3,824
Loreto	1,225	1113	2,078
Madre de Dios	2,695 9	32 1	,487
Moquegua	1,380 1	470	1,593
Pasco 3	11	436 7	59
Piura	3,854 6	206	14,503
Puno	3,229	813	1,378
San Martín	1,837 9	85	4,403
Tacna 5	85 1	81 8	45
Tumbes	4,466 4	864	8,795
Ucayali	304 2	52 6	78
Total	99,768	99524	135,938

Nota. Elaboración extraída del Anuario Estadístico PNP (2020, 2021, 2022).

Explorando la problemática, Díaz y Obillus (2022) determinaron que el CIP afectó la libertad de las personas de Lima Norte en la pandemia Covid-19, apreciándose casos que superaron el lapso de las 4 horas de restricción, levantamiento de actas sin motivación o estándares de ley, tecnología deficiente que no contribuyó a una pronta identificación, existe débil apego por observar los presupuestos del artículo 205 y los actos policiales de identificación no ocurren in situ quebrantando el ordenamiento legal.

Por su parte, Huamán (2022) señaló que el CIP no contribuye a la identificación de extranjeros, siendo deficiente la información que tiene al respecto la Superintendencia Nacional de Migraciones. Al respecto, se reportó que un número significativo de inmigrantes no portan o disponen de documentación lícita, lo cual dificulta el CIP, resultando el plazo de 4 horas insuficiente para cumplir con el rol identificativo, lo cual es una limitación

para enfrentar la lucha contra el crimen sabiéndose la participación activa de ciudadanos extranjeros; a la vez, que el Protocolo por CIP preconizado en el 2018 por el Ministerio de Justicia y Derechos Humanos no es útil para tal cometido ya que no se adapta a la praxis real.

Talavera (2021) refiere que el CIP debe actuarse con justificación fáctica y/o probatoria mínima vinculada a prevención o investigación delictual, evitando operativos aparentes con matices de corrupción, así como no instituir la detención por sospecha o invertir el principio de presunción de inocencia por culpabilidad. Asimismo, la facultad discrecional policial no corresponde a detención de ciudadanos de manera incausada y requerir documento de identidad, sino que el acto restrictivo debe ser idóneo, necesario y proporcional, garantizando el derecho a la presunción de inocencia y plazo razonable. Para Arimborgo y Zapata (2020) la actuación por CIP generaba vulneración al derecho a la libertad personal, puesto que el conocimiento sobre el procedimiento y diligencias del personal policial por el CIP no era idóneo, aplicándose deficientemente, con errónea interpretación y aplicación del artículo 205, evidenciando afectación de derechos en personas intervenidas.

Duce y Lillo (2020) refiriéndose a Chile, precisan que en el periodo de 2009 a 2018 se produjeron 25 millones de actos por CIP, abarcando unos 2,5 millones de casos por año. Estos controles se realizan de manera preventiva, por lo que es usual la actuación del CIP sin sospecha, sin embargo, se carece de publicación de información que permita conocer la eficacia de tal procedimiento y de esa forma evaluarlo y optimizarlo, puesto que no existe información sobre qué ocurre en las 8 horas del control identificativo, no se conoce cuáles son los elementos indiciarios que justifican el CIP, no existe data respecto a los registros de vestimentas, equipajes o vehículos, focalizándose algunas veces el accionar policivo en grupos vulnerables. Por su parte, Sánchez y Ureta (2017) indican que en el modelo chileno el CIP resulta problemático ya que está en cuestión los derechos fundamentales del viandante y el actuar policiaco, se considera que el CIP ya sea preventivo o investigativo es una detención por restringir la libertad, el CIP preventivo tiene resabios de detención por sospecha (por su forma vestir, tez, actitud, higiene personal, etc.), es decir, identificación sin motivación idónea, mientras que el CIP investigativo sí corresponde a indicios que vinculan a un sujeto con un hecho criminoso. Se postuló que anualmente 1.800.000 ciudadanos son objeto de CIP lo cual representa un 10% de la población chilena.

Según Paredes (2019) se determinó que la actuación del personal policial de las Comisarías generaba múltiples problemas frente al CIP, no siguiendo los alcances procedimentales del artículo 205 de la Ley de enjuiciamiento criminal y normas reglamentarias en el Perú. Los problemas identificados corresponden a la deficiente claridad en el documento de identidad a presentar, lo que limita la actuación de los policías única y exclusivamente a aceptar la presentación de DNI. Asimismo, se conoce la existencia de casos deficientes en identificación policial que generaron cuestionamientos al actuar policivo y el proceso penal.

Es importante comprender que el Control de Identidad Policial (CIP) es una figura relevante en el ordenamiento legal peruano, empero, existe una brecha entre lo precisado en el artículo 205 del estatuto procesal penal y la praxis que ejecutan todos los días los policías de prevención e investigación en el Perú. Tal cuestión, quedó reflejada con el caso 12.982 de la Corte, dónde se demostró vulneración de derechos por tal acto; por un lado, existe la creencia de que el artículo 205 es totalmente nítido o claro y que no requiere reglamentación o variación alguna, mientras que, en el otro escenario, la realidad demuestra que hay muchas cosas por hacer, de tal forma que los ciudadanos tengan la plena seguridad que sus derechos fundamentales no serán vulnerados por una mala praxis del CIP.

Legalidad del control de identidad policial

El estudio del CIP en el modelo peruano es débil, si aproximamos la búsqueda de información al respecto, encontraremos que son nulos los adentramientos doctrinarios, existen datos aislados y minúsculos en algunos textos, no obstante, la práctica policiaca del CIP ocurre los 365 días del año a lo largo y ancho de la patria, con especial eco en los «operativos policiales» que se desarrollan en calles y avenidas, en algún espacio o momento de las 24 horas, ya sea en el invierno, otoño, primavera o verano.

En la historia el órgano policial siempre ha tenido la «atribución» de identificación de las personas, existió una época en la cual se intervenía a sujetos llamados «vagos» encontrados en la vía pública, acorde a la Ley N° 4891 sobre la vagancia en vigencia del 18 de enero de 1924 al 12 de mayo de 1986, obviamente el poder de policía de aquellos tiempos era muy fuerte, lo cual ahora no se adaptaría por afectar derechos fundamentales.

Muchos operadores de justicia dudan sobre la constitucionalidad del CIP, existen posiciones de ambos lados, algunos afirman que es una atribución policial constitucional bajo el amparo del artículo 2.24.b, otros refieren que es inconstitucional, ya que la Carta Magna no permite afectación de la libertad personal más allá del artículo 2.24.f, confundiendo detención policial por flagrancia con restricción de la libertad por CIP; tal era la «presunta inconstitucionalidad» que en su momento se presentaron sendos proyectos de leyes —PL en adelante— para derogar el artículo 205 de la norma adjetiva, así lo encontramos en: (i) PL 11710/2004-CR del 15 de octubre de 2004; (ii) PL 11722/2004-CR del 18 de octubre de 2004; (iii) PL 11739/2004-CR del 19 de octubre de 2004; (iv) PL 11826/2004-CR del 29 de octubre de 2004; y (v) PL 11949/2004-CR., del 16 de noviembre de 2004.

El CIP es constitucional en el Perú, su fundamentación jurídica está en el artículo 2.24.b, permitiéndose la «restricción» de la libertad personal en base a una ley. El derecho a la libertad individual no es ilimitado, existe la posibilidad de restricción, así el Tribunal Constitucional reconoció que su «ejercicio no es absoluto ya que puede ser restringido», entonces, no toda privación o restricción de la libertad tiene rasgos inconstitucionales ya que se puede coartar legítimamente (Expediente 03425-2010-HC y Expediente 05765-

2009-HC).

En el marco legal supranacional de carácter vinculante las limitaciones de la libertad personal, llámese «restricciones», se encuentran nítidamente fundamentadas o desarrolladas, así tenemos que en: (i) la Declaración Universal de los Derechos Humanos la restricción encuentra ligazón con la «moral, orden público y bienestar general» (artículo 29); en el Pacto Internacional de Derechos Civiles y Políticos la restricción se relaciona con la «seguridad nacional, orden público, salud, moral pública» (artículo 12); en la Convención Americana sobre Derechos Humanos la restricción se relaciona con «prevención de infracciones penales, seguridad nacional, seguridad o el orden público [para nosotros intrínsecamente seguridad ciudadana], moral y salud pública» (artículo 22).

El CIP observa principios de obligatorio cumplimiento, a saber: (i) el principio de intervención mínima o necesidad está referido al caso en específico o hechos de actuación policial idóneos; (ii) el principio de razonabilidad se refiere a la justificación lógica en el acto policial; (iii) el principio de proporcionalidad o prohibición en exceso que observa coherencia y equilibro del policía frente al viandante; y (iv) el principio de primacía de la persona humana y sus derechos fundamentales se decanta por su propia expresión «el respeto al ser humano, por sobre todas las cosas, está primero», claro está con raigambre en el Decreto Legislativo N° 1267, todos estos principios vinculados a cuestiones de prevención o investigación delictual [averiguación de un hecho punible].

Figura 1

Legitimidad del CIP.

Nota: Normativa asociada a la legalidad del CIP.

La jurisprudencia de la Corte Interamericana de Derechos Humanos ha precisado que cualquier restricción debe reunir el aspecto material (causas fijadas en la Constitución y la Ley) y aspecto formal (procedimientos objetivamente definidos), el ordenamiento legal peruano sí reúne tales presupuestos, a saber: (i) Aspecto material: Carta Magna, arts. 2.24.b y 166; Decreto Legislativo N° 1267, arts. III, 2.7 y 3.2, (ii) Aspecto formal: Decreto

Legislativo N° 957, art. 205; Protocolo de CIP 2018, respecto al aspecto formal se postula que el órgano policial redacte la «Directiva policial de restricción por Control de identidad policial», delineando la actuación procedimental del policía interviniente, policía de identificación y demás de índole policiaco (Corte Interamericana de Derechos Humanos [CIDH], 2006, 2012, 2016).

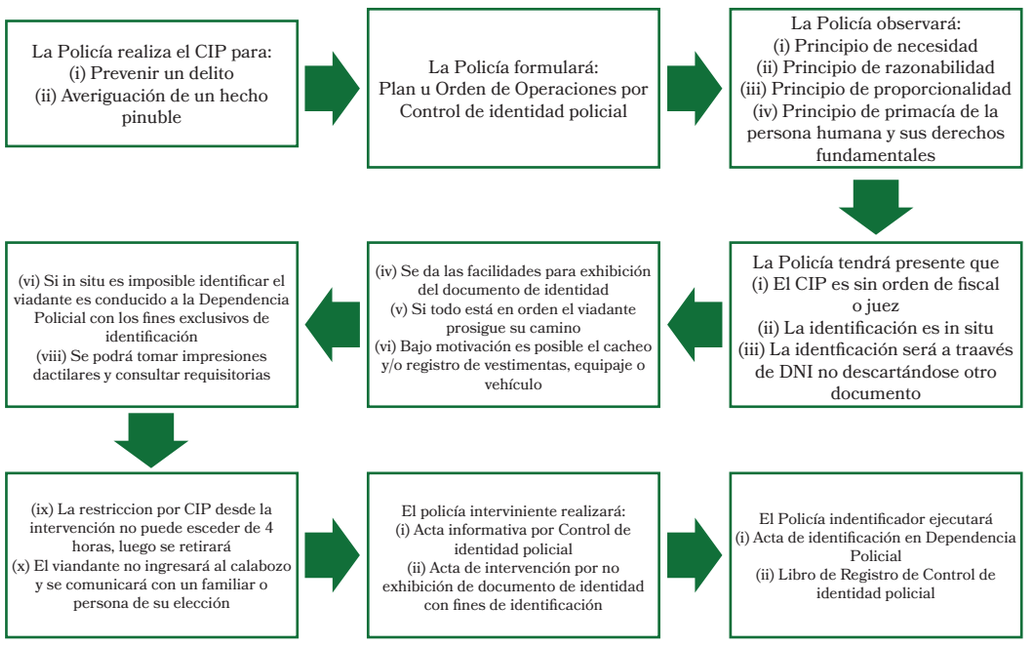
En el contexto internacional, la figura del CIP como tal existe solamente en la realidad chilena, específicamente, en el artículo 12 (Control de identidad preventivo) y artículo 85 (Control de identidad investigativo) de la Ley de enjuiciamiento criminal chilena del 2000, infiriéndose en su génesis la influencia mapochina en la realidad inca del 2004, empero, en Chile se han hecho múltiples reformas moldeando tal actuación cosa que no ha replicado el Perú hasta nuestro días, así tenemos, Ley N° 19.567, Ley N° 19.693, Ley N° 19.696, Ley N° 19.942, Ley N° 20.253, Ley N° 20.931 (Enriquez et al., 2021).

Los procedimientos policivos chilenos con fines de identificación in situ no deben exceder el plazo de 1 hora y en caso no lograrse el viandante seguirá su camino (artículo 12); cuando no es posible acreditar la identidad o se niega el viandante es conducido a la unidad policial por el plazo no superior a 8 las horas, exclusivamente con fines de identificación (artículo 85), los documentos que facilitan la identificación allá son cédula de identidad, licencia de conducir, pasaporte, tarjeta estudiantil, cualquier dispositivo tecnológico (Enriquez et al., 2021a).

¿El resto de policías extranjeros no ejecutan el acto preventivo-restrictivo? Sí, pero con reglamentación legal de talante policiaco bajo el poder de policía del Estado, en España, la identificación de sujetos sospechosos en los artículos 493 y 770 de la Ley de enjuiciamiento criminal española, identidad de ciudadanos en los artículos 8, 9, 16, 17, 18, 19, 20 de la Ley Orgánica N° 4/2015 de seguridad ciudadana; en Uruguay, el deber de identificarse se ubica en el artículo 50 de la Ley N° 18.315 Procedimiento Policial [ver Ley N° 19.889]; en Argentina, para conocer la identidad se desarrolla en el artículo 15 de la Ley 13482 de Organización de las Policías; en México, existe el control preventivo provisional en base a la norma constitucional, artículo 21, desarrollado jurisprudencialmente por la Suprema Corte de Justicia de la Nación (Amparo directo en revisión: 3463/2012, 1596/2014; Acción de inconstitucionalidad: 10/2014 y 11/2014); en Colombia, artículos 35.3, 157, 158-160 de la Ley 1801 Código Nacional de Policía y Convivencia (Enriquez et al., 2021b).

Figura 2

Procedimiento genérico por CIP.



Nota: Se presenta el proceso policial para el CIP.

En el Perú, el artículo 205 precisa que la identificación es a través del "documento de identidad", no dice Documento Nacional de Identidad (DNI), consideramos que bajo una interpretación extensiva corresponde a cualquier documento que facilite el acto de identificación que es labor en sí del órgano policivo dotado de las herramientas idóneas, entonces, resulta válida la apreciación razonable de licencia de conducir, libreta militar, partida de nacimiento o cualquier otro documento público o privado (Resolución N° 029-2005-MP-FN; Protocolo de CIP 2018); empero, también debería tenerse presente que el DNI es el documento oficial para aspectos identificatorios (artículo 30 de la Ley N° 26497).

Se debe agregar que, el 5 de octubre de 2023, se publicó en el Diario Oficial El Peruano el Decreto Legislativo N° 1574, única modificación hasta el momento del artículo 205 del estatuto procesal penal, empero, tal marco legal obedeció a delinear aspectos respecto al control de identidad de ciudadanos extranjeros, así tenemos que sobre las horas de restricción se ratificó que el procedimiento policivo con fines de identificación frente a ciudadanos nacionales no puede exceder de 4 horas, pero, específicamente, ante a ciudadanos extranjeros no puede superar las 12 horas.

El primer caso por CIP ante la Corte

El caso 12.982 Azul Rojas Marín y otra versus Perú del 2020 es el «primer caso por CIP» que lamentable llegó a la Corte Interamericana de Derechos Humanos, la deficiente actuación policial desencadenó en sanción para el Estado Peruano y demás; en sus diversas páginas la Corte desentrañó las series y múltiples anomalías que existen en torno al CIP, dentro de ellas la falta de planificación, desconocimiento de roles de actuación, cómo intervenir por razones de orientación sexual, la falta de información al viandante, etc.

El 12 de marzo de 2020, la Corte Interamericana de Derechos Humanos, emitió sentencia sobre el Caso Azul Rojas Marín y otra versus Perú, Caso 12.982, determinando fehaciente y contundentemente que el Estado Peruano violó la Convención Americana sobre Derechos Humanos, artículos 5.1, 5.2, 7.1, 7.2, 7.3, 7.4, 8.1, 25.1, entre otros, además, la Corte precisó daño inmaterial a los agraviados, fijando reparación pecuniaria de USD$ 60.000,00 (sesenta mil dólares) para Azul Rojas Marín y USD$ 15.000,00 (quince mil dólares) para Juana Rosa Tanta Marín.

En resumen, la data histórica del Caso 12.982 indica que el 25 de febrero de 2008 agentes policivos de la Comisaría de Casa Grande (Ascope-La Libertad) conocieron de la presencia de tres sujetos desconocidos por la urbanización Miguel Grau, logrando la intervención de uno de ellos (sospechoso) quien presentaba síntomas de embriaguez y no portaba documentación alguna para su identificación por lo cual procedieron al registro personal sin encontrar ningún objeto ilícito u otro de interés delictual, siendo conducido a la Comisaría con fines de identificación, empero, después no se encontró registro alguno sobre tal actuación por CIP conforme lo establece el artículo 205 de la norma adjetiva, la Corte ordenó que el Estado Peruano (ítem 268) no aplique el artículo 205 del Código Procesal Penal de “manera abusiva y discriminatoria”.

Sobre la información por CIP, por ejemplo, si un viandante no tiene documento de identidad, se agota su identificación en el lugar de intervención no logrando su cometido, conforme al artículo 205 del digesto procesal penal debe ser conducido a la unidad policial con fines de identificación hasta un plazo máximo de 4 horas, en ese escenario ¿el viandante debe ser informado de sus derechos? Consideramos enfáticamente que sí, así como ocurre con una persona detenida por flagrante delito se le informa sus derechos establecidos en el artículo 71 del CPP tan igual al viandante por restricción se le debe hacer conocer su derechos en armonía con el artículo 7.4 de la Convención Americana sobre Derechos Humanos [así lo determinó la Corte], luego será trasladado a la dependencia policial, en tanto se restringirá su libertad conforme a ley el policía debe formular la novísima «Acta informativa por CIP», esto fue advertido en el caso 12.982 [no ocurrió] y debe ser implementado para evitar cuestionamientos a la labor policiva ya que actualmente el Protocolo de CIP 2018 no precisa nada al respecto, empero, es incuestionable por fundamentos de hecho y derecho que la policía trabaje con tal instrumento legal propuesto que debe ser considerado en el marco normativo policivo prontamente porque así lo

determinó la Corte bajo amparo de ley.

Prevención delictual

La función de prevención policial encuentra fundamentación jurídica en el artículo 166 de la norma constitucional. Una de las aristas del CIP corresponde a la prevención ejecutada por el órgano policial en su real dimensión, muchas veces a través de «operativos policiales», estas son acciones planificadas que se ejecuta a favor de la prevención delictual, prevenir es anticiparse a posibles escenarios delictuales empleando recursos humanos y herramientas logísticas que buscan evitar tales sucesos o problemas, la prevención es proactiva cuando la policía se adelanta a escenarios de probable actividad delincuencial y es prevención proactiva cuando producido el hecho delictivo se ejecutan acciones a fin de evitar repetición o reincidencia de tales actos (De León-Escribano et al., 2004).

La prevención delictual eficaz al 100% no existe, lo que un Estado busca es su control razonable, la eliminación por siempre del delito es una utopía [quisiéramos que fuera diferente], prevenir no engloba únicamente perseguir y sancionar, es esencialmente conocer las causas del problema criminal ya que el crimen es una temática social y comunitaria, la ley preventiva debe ser acompañada y articulada por sus líderes y la comunidad en general, es tarea de todos, la prevención policial en solitario no logrará su cometido si no existe involucramiento de autoridades y ciudadanía, así lograremos disminuir la criminalidad ya que una idónea política criminal estudia concienzudamente la prevención y reacción frente al acto delictual (GarcíaPablos, 1994).

¿El acto de prevención policial debe estar en el Decreto Legislativo N° 957? Apreciamos que no, ya que la ley de enjuiciamiento criminal peruana tiene su génesis en la notitia criminis y no en el acto de prevención, si claro podría existir casos excepcionales de virar de prevención al delito. Sin embargo, resulta extraño porque el legislador incorporó cuestiones preventivas en la norma adjetiva creando con ello ejes problemáticos. Al respecto, conforme se precisó en Latinoamérica los únicos países que tienen la figura del CIP como tal son Chile, Perú y Uruguay, empero, este trasladó tal figura a la Ley N° 18.315, Procedimiento Policial, las legislaciones mayoritariamente no tratan el acto preventivo en la norma procesal penal, sino en norma policiaca vinculada al poder de policía: Estado.

El digesto procesal penal peruano no debe tratar sobre prevención del delito (Oré, 1993), existen posiciones abiertas que el CIP debe registrarse en norma aparte distinta al procesal penal (Duce y Riego, 2009; Gálvez, 2017; Mavila, 2005; Gálvez et al., 2008), sobre esto último guardamos armonía ya que consideramos que efectivamente el CIP debe estar en una ley especial de índole policial, como ocurre en España, Uruguay, Colombia y otros, bajo el título tentativo quizás de «Ley de restricción por CIP».

Los «operativos policiales» por CIP no se realizan o fueron diseñados para molestar a los viandantes por no portar físicamente su CIP, pese a que según la Ley N° 26497 el uso de Documento Nacional de Identidad es obligatorio (artículo 30), tal acto es con

fines de identificación, para ello el Estado Peruano debe proveer los sistemas biométricos respectivos, actualmente, es imposible ver en el campo a policías con estaciones móviles de captura en vivo o equipos portátiles de identificación rápida, es decir, la identificación se hace a «ojo de buen cubero», hecho que debe absolverse prontamente.

La ejecución de «operativos policiales» es relevante en la función policial, empero, no se conoce de marco normativo específico, llámese «Plan u orden de operaciones de CIP» por cada sector de responsabilidad de comisarías o DIVINCRIS, sabiéndose que esta actividad se ejecuta todo el año, por ende debe ser planificada [doctrina de Estado Mayor], en tanto, sus insumos deben ser el mapa del delito, las zonas rojas, calles y avenidas principales de alto tráfico vehicular y peatonal, perfiles delincuenciales, puntos peligrosos, etcétera; también debe existir una «Directiva policial por CIP» que detalle pormenorizadamente la actuación policiaca por CIP, el marco normativo de intervención, el rol del policía interviniente, rol del policía de identificación, los cuadernos o registros, las actas, entre otros, ya que el Protocolo de CIP 2018 no alcanza tales expectativas.

El registro

El registro en el CIP es otro eje problemático álgido de urgente solución. En los «operativos policiales» se busca identificar a las personas, con fines preventivos o averiguación de un delito, en ese contexto, suelen ocurrir registros de personas vestimentas, equipaje o vehículos, hecho que es muy criticado, en tanto, no existiría una regulación legal idónea al respecto, confundiéndose el «registro de personas» con el «registro superficial o cacheo», es decir, el matiz investigativo del primero y el preventivo del último.

En el Diccionario de la lengua española (Real Academia Española, 2015), registro es la acción de registrar, entendida como (i) Mirar, examinar algo con cuidado y diligencia; (ii) Examinar algo o a alguien, minuciosamente, para encontrar algo que puede estar oculto; en el Decreto Legislativo N° 957 se encuentran los términos «registro» (artículo 68.c), «registrarle» (artículo 205.3) y «registrarla» (artículo 210.1), vinculados al registro de personas, vestimentas, equipaje o vehículos, no apreciándose las diferencias, ¿cuándo tal registro es un acto de prevención o investigación?, esto ocasiona que la mayoría de operadores de justicia se enfoquen en la existencia única del «registro de personas» del artículo 210 relacionándolo sinonímicamente con el artículo 205, es decir, las mismas reglas investigativas con las preventivas, aspecto muy controversial de débil estudio en la realidad peruana.

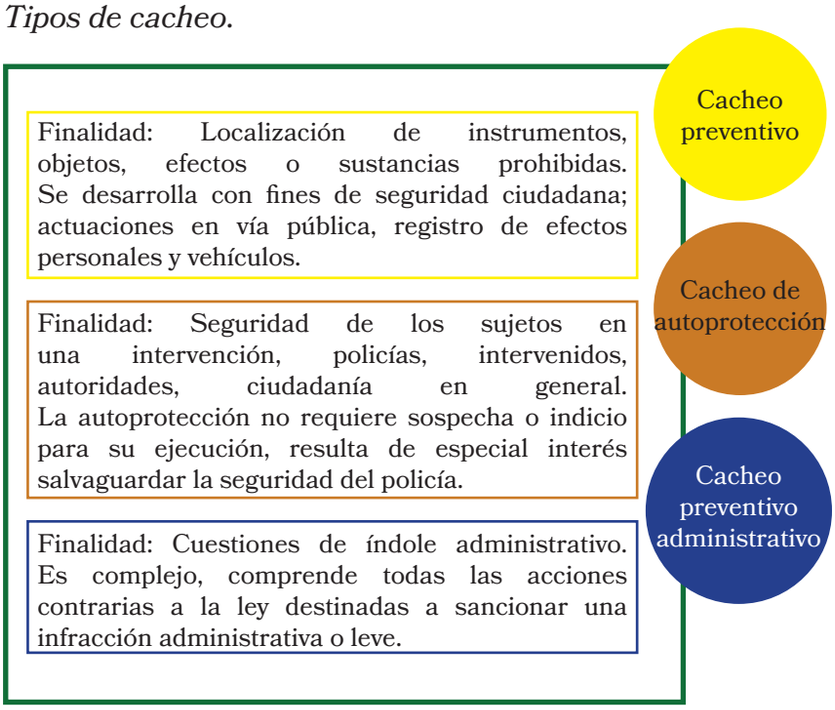
La doctrina según el Manual de Procedimientos Operativos Policiales de la Policía Nacional del Perú, aprobado con Resolución Directoral N° 030-2013-DIRGEN/EMG, del 15 de enero de 2013, indica que el cacheo «es un registro rápido de la persona sospechosa a fin de buscar armas lo suficientemente grandes para poderlas detectar a través de las ropas». Sin embargo, nuevamente surge la interrogante en prevención o investigación, sabiéndose que el artículo 210 exige que se pregunte al intervenido sobre el «bien buscado», empero, en cuestiones de prevención el policía no sale a buscarlos, entonces,

como se podría «invitar a que exhiba y entregue el bien buscado» a un viandante por cuestiones preventivas, lamentable confusión del legislador.

La ley y doctrina se olvidó del registro superficial o cacheo de fuente española, al respecto existe mucho por desarrollar, compete al órgano policial profundizar en la cuestión, ya que el registro de personas no es sinónimo del registro superficial o cacheo. Debe apreciarse que el registro del artículo 210 se refiere a una investigación y el registro del artículo 205 se refiere a prevención, este denominado también «registro superficial por palpación», «cacheo» o «cacheo policial».

Figura 3

Tipos de cacheo.



Nota: Elaboración en base a Guillén 2016, «La Práctica del Cacheo en el Sistema Constitucional Español».

Por otra parte, también en el contexto del cacheo se carece de mayor abundamiento sobre la temática del «registro preliminar» y «registro definitivo», ambos vinculados a la doctrina de investigación criminal, siendo que el primero es en el lugar de los hechos y el segundo en la unidad policial, sostenidos el uno y el otro con idónea motivación; conviene subrayar que, sobre la sobre la prolongación del registro personal la Casación 253-2013-Puno, ilustró que ocurre cuando: (i) No existan garantías para la integridad del fiscal y policías, (ii) Riesgo por exacerbación de personas que presencian e impiden el acto y (iii) Razones suficientes que sustenten en mantener y conseguir el objetivo de la actuación. Asimismo, el Recurso de Casación N° 2752-2021, La Libertad, precisó que: «No está disciplinado, y no puede estarlo, que el acta necesariamente se levante en el mismo lugar

del suceso materia de intervención. Ello depende, desde luego, de las circunstancias del caso» (Enriquez, 2022).

Policía interviniente, retenciones, instructor policial y buen trato

Ante la ausencia de instrumentalización legal del actuar policial bajo estándares del novísimo proceso penal, tanto en el área de prevención como de investigación criminal, los policías recurren a ideas múltiples para cubrir determinados actos policiales, muchas veces muy bien intencionados, empero, no cubren o satisfacen las exigencias de ley, varios de ellos vinculado al CIP, cuestión que buscaremos absolver a continuación.

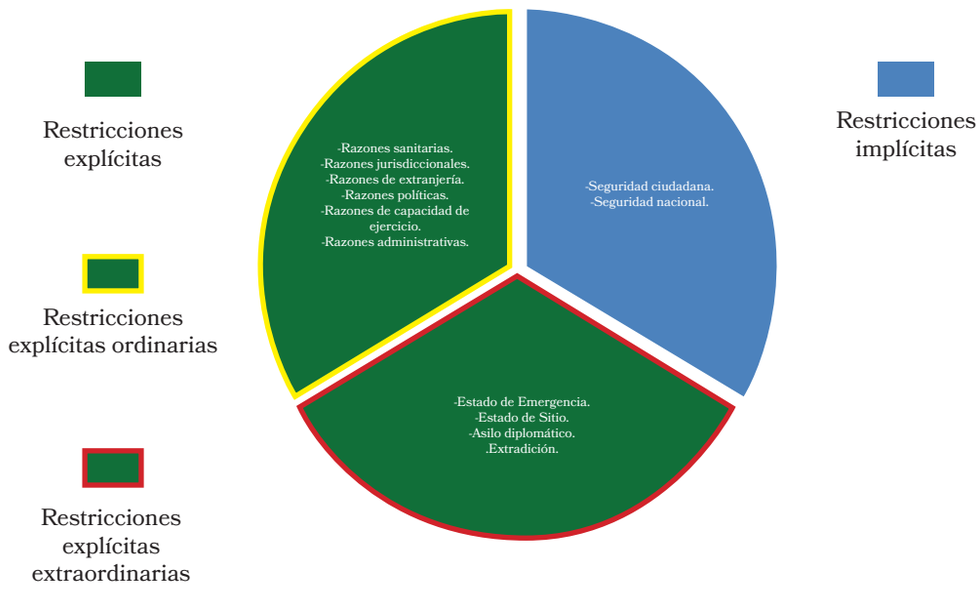
Sobre el policía interviniente, en el modelo peruviano no es la "Primera Autoridad Respondiente", del modelo colombiano o el "Primer Respondiente" del modelo mexicano, acá corresponde a "Policía interviniente", así se reconoció nuestro aporte en la Resolución Directoral N° 600-2015-DIRGEN/EMG-PNP del 2015 (Directiva para actuar en delito flagrante por cohecho activo genérico) y Resolución Directoral N° 135-2016-DIRGEN/EMG-PNP del 2016 (Directiva para actuar en flagrante delito). Por lo que, el policía interviniente, es el agente que ejecuta una intervención en el lugar del hecho, recayendo tal actuación en un efectivo de cualquier especialidad que realiza la inicial actuación frente a un acto preventivo o investigativo.

Sobre las retenciones, tal figura está reconocida en el artículo 209 de la norma adjetiva, siendo útil para practicar una pesquisa y que determinado sujeto no se ausente del lugar de actuación por el término de 4 horas. No obstante, por esto último (4 horas) algunos interpretan que el artículo 209 es sinónimo del 205, cuando este es con finalidad preventiva o averiguación de un hecho delictual y aquel es una pesquisa, el CIP es una restricción conforme al artículo 2.24.b de la Carta Magna desarrollado en el artículo 205 del estatuto procesal penal, por el art. 209 el sujeto se queda "inmóvil" por 4 horas, por el art. 205 si resulta imposible la identificación del ciudadano es conducido a la unidad policial, no se queda "inmóvil", notoria diferencia en la praxis.

Esta confusión del artículo 205 con el 209, sigue hasta nuestros días, el Decreto Supremo N° 002-2023-MIMP del 8 de febrero de 2023, definió a la retención policial como «Limitación temporal en el desplazamiento de una persona con fines de identificación o cuando resulte necesario que se realice una investigación o pesquisa», con ello se creó una nueva figura, desnaturalizando y confundiendo una vez más la actuación del CIP con el de una pesquisa; la retención está vinculado con impedir el movimiento de una persona, en el CIP el sujeto está en movimiento y podría ser trasladado a una unidad policial, infiriéndose débil adentramiento al estudio de las restricciones en nuestro país, la restricción no es sinónimo de retención, la restricción por el CIP es una restricción implícita vinculada a la seguridad ciudadana, la retención es una pesquisa de talante investigativo.

Figura 4

Tipos de restricción



Nota: Elaboración propia en base al Expendiente 2876-2005-HC.

Sobre el instructor policial, la documentación policial todavía tiene resabios del modelo inquisitivo, mientras que la reforma procesal penal dejó atrás el Código de 1940 por el Código de 2004, todavía los policías perviven mencionando tal nombre respecto al policía que suscribe los múltiples actos de investigación, cuando la instrucción ya no existe, la instrucción es de 1940, hoy, tal denominación cambió, ahora es policía interviniente, policía de investigación, policía de identificación, entre otros, son las enunciaciones acordes y corresponden al cambio de mentalidad que urge adoptar.

Sobre el buen trato, los policías redactan en su actuación la «constancia de buen trato», tal documento no está en ningún extremo del Código Procesal Penal, es un calco del modelo colombiano (parte final del Acta de derechos del capturado, FPJ 6) que tiene otro talante, es más el Protocolo por CIP en el procedimiento 18 lo detalla «elaborar una constancia de buen trato», empero, se olvidaron precisar su formato y en qué consiste dejándolo al libre albedrio, en la praxis se dice de un trato físico y psicológico, lo cual es ajeno al policía que no es ni médico para afirmar problemas del cuerpo humanos ni es psicólogo para afirmar aspectos de la conducta y la mente, sabiéndose que el funcionario policial en observación a su Ley cumple siempre el «Principio de primacía de la persona humana y sus derechos fundamentales», es decir, el respeto al ser humano primero, siendo irrelevante levantar tal documento bajo el supuesto que evitará y demostrará defenderse sobre un posible exceso policial (Enriquez y Arroyo, 2020).

Conclusiones

Existen problemas con la actuación por el CIP que tiene dos vertientes, talante preventivo e investigativo, no diseñándose a la fecha un marco legal idóneo diferenciador de ellos, que recoja también el aprendizaje en torno a la sentencia que sancionó al Estado Peruano por el primer caso de CIP que llegó a la Corte Interamericana de Derechos Humanos, caso 12.982, empero, es lícito en el Perú al amparo de la Carta Magna, arts. 2.24.b y 166; Decreto Legislativo N° 1267, arts. III, 2.7 y 3.2 (Aspecto material) y Decreto Legislativo N° 957, art. 205; Protocolo de CIP 2018 (Aspecto formal).

La actuación preventiva no debería estar en el digesto procesal penal peruano, el acto de prevención no es sinónimo de noticia criminal, debe existir norma aparte. No obstante, el CIP debe seguir aplicándose en armonía del artículo 205 y el aprendizaje del caso 12.982, postulándose al respecto el empleo de la novísima «Acta informativa por CIP», frente al acto de restricción de la persona, cuestión de urgente aplicación en la praxis policiva a nivel nacional.

El registro de personas del artículo 210 de la ley de enjuiciamiento criminal peruana no es igual al registro de vestimentas, equipaje o vehículo del artículo 205, aquel es con fin investigativo y este con fin preventivo, no hay un desarrollo del «cacheo» de tradición española, faltando reglamentar también el registro preliminar en el lugar del hecho y el registro definitivo en la unidad policial, ambos con motivación y estándares de ley.

Referencias

Arimborgo, A., y Zapata, J. (2020) Vulneración del derecho a la libertad personal y control de identidad policial, en intervenidos indocumentados, distrito San Mateo – Huarochirí [Tesis de pregrado, Universidad Peruana Los Andes]. http://www.repositorio.upla.edu.pe/bitstream/handle/20.500.12848/2041/TESIS%20%20ARCO%20y%20AMES.pdf?sequence=1&isAllowed=y

Corte Interamericana de Derechos Humanos (2006). Caso Servellón y otros vs. Honduras, (Fondo). Sentencia de 21 de septiembre de 2006.

Corte Interamericana de Derechos Humanos (2012). Caso García y familiares vs. Guatemala, (Fondo). Sentencia de 29 de noviembre de 2012.

Corte Interamericana de Derechos Humanos (2016). Caso Herrera Espinoza y otros vs. Ecuador, (Fondo). Sentencia de 1 de septiembre de 2016.

De León-Escribano, C. (2004) Manual de Seguridad Preventiva y Policía Comunitaria. Instituto de Enseñanza para el Desarrollo Sostenible y National Endowment for Democracy. https://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/556D247E5000992A05257F480064B81C/$FILE/manual_policias_comunitaria_guatemala.pdf

Duce, M., y Lillo, R. M. (2020). Controles de identidad realizados por Carabineros: Un aproximación

empírica y evaluativa sobre su uso en Chile. Revista de Estudios de la Justicia, 33, 167–203. https://doi.org/10.5354/0718-4735.2020.57635

Duce, M. y Riego, C. (2009). Proceso Penal. Santiago: Editorial Jurídica de Chile.

Díaz W., y Obillus, R. (2022) El control de identidad policial y la libertad personal como derecho fundamental de los intervenidos en pandemia covid-19 [Tesis de pregrado, Universidad César Vallejo].

Enríquez, J. (2022). Dogmática del cacheo policial. Chapqa, 2(1), 7-29. https://revistachapqa.com/index.php/e/article/view/25

Enríquez, J., y Arroyo, I. (2022). El ABC del funcionario policial en el novísimo proceso penal peruano. AC Ediciones.

Enríquez, J., Arroyo, I., y Julca, M. (2021). Control de identidad policial. Privación o restricción de la libertad personal. AC Ediciones.

Gálvez, T. (2017). Medidas de coerción personales y reales en el proceso penal. Conforme a la modificación constitucional de derechos legislativos. Ideas Solución Editorial.

Gálvez, T., Rabanal, W., y Castro, H. (2008). El Código Procesal Penal. Comentarios descriptivos, explicativos y críticos. Jurista editores.

García-Pablos, A. (1994). Criminología. Una introducción a sus fundamentos teóricos para juristas (2da edición). Tirant Lo Blanch.

Huamán, J. (2022) El control de identidad policial en migrantes extranjeros que realiza la BICEC-DIRINCRI PNP en Lima Metropolitana, 2020-2021 [Tesis de pregrado, Universidad César Vallejo]. https://repositorio.ucv.edu.pe/handle/20.500.12692/105621

Maldonado, J. (2018) Metodología de la investigación social. Paradigmas: cuantitativo, sociocrítico, cualitativo, complementario. Ediciones de la U.

Mavila, R. (2005). El Nuevo Sistema Procesal Penal. Jurista Editores.

Ministerio de la Mujer y Poblaciones Vulnerables (2023). Decreto Supremo que aprueba el Protocolo de actuación conjunta del Estado para la articulación de servicios de atención a víctimas de delito, retenidas, liberadas o rescatadas en el ámbito de peruanas o extranjeras que ejercen la prostitución.
https://www.gob.pe/institucion/mimp/normas-legales/3878/712-202-2023-mimp

Náupas, H., Valdivia, M., Palacios, J., y Romero, H. (2018). Metodología de la investigación. Cuantitativa, cualitativa y redacción de la tesis (3ta edición). Ediciones de la U.

Paredes, A. (2019) Uso indebido del control de identidad por parte de la Policía Nacional de Perú y mecanismos para su aplicación adecuada [Tesis de maestría, Universidad Nacional de Cajamarca]. https://repositorio.unprg.edu.pe/bitstream/handle/20.500.12893/7472/BC-TES-M2.7370%20

PAREDES%20BRUNO.pdf

Policía Nacional del Perú. (2015). Directiva para la intervención e investigación policial, en delito flagrante, por medio operativo agrario [Resolución Directoral 600 del 7 de agosto].

Resolución Directoral Nº 135-2016-DIRGEN/EMPG-PNP (2016) Que aprueba la Directiva para la Intervención Policial en Delito Flagrante de Actas elaboradas por una Comisión Legislativa integrada por representantes de las Unidades Policiales y el Ministerio Público. https://img.gob.pe/images/LEGIS.PE-Directiva-Para-la-Intervenci%C3%B3n-policial-en-Flagrante-delito.pdf

Policía Nacional del Perú (2020). Anuario estadístico policial 2020. https://www.policia.gob.pe/estadisticoanp/anuario-2020.html

Policía Nacional del Perú (2021). Anuario estadístico policial 2021. https://www.policia.gob.pe/estadisticoanp/anuario-2021.html

Operaciones psicológicas en la ejecución de actuaciones policiales

Russell Laudrup Casimiro Dionicio

Román Jesús Marquina Luján

María Moreno Jorge

Escuela de Posgrado de la Policía Nacional del Perú

Introducción

Durante más de dos mil años, las operaciones psicológicas han sido utilizadas como una estrategia previa a los enfrentamientos armados, con el propósito de infundir miedo en el enemigo. Sin embargo, fue a partir de la Segunda Guerra Mundial cuando se emplearon de manera planificada y organizada, aplicando una amplia variedad de recursos para alcanzar los objetivos militares del país que las implementaba. Con el tiempo, su uso se extendió a actores estatales y no estatales, especialmente en contextos policiales y políticos, donde las operaciones psicológicas podían tener efectos benéficos o perjudiciales en los conflictos y en la percepción pública (Rodman, 2012).

Según la definición de la Organización del Tratado del Atlántico Norte (North Atlantic Treaty Organization [OTAN], 2003), las operaciones psicológicas son "el conjunto de accione psicológicas debidamente planificadas en tiempos de paz, crisis y/o guerra, orientadas a influir en los comportamientos y emociones de enemigos, amigos y neutrales, con el fin de afectar el logro de objetivos militares y políticos" (p. 3). Esto implica llevar a cabo acciones de acercamiento, sensibilización, apoyo social, entre otras actividades, con el objetivo de influir en la comprensión de una crisis o conflicto, gestionando las percepciones de las audiencias objetivo, así como sus emociones, actitudes, motivaciones, razonamientos y, especialmente, sus comportamientos y decisiones (Vázquez, 1998; Departamento de Ejército, 2003; OTAN, 2007; Vejvodová, 2019).

Por su parte, las operaciones policiales se presentan como un conjunto de acciones que realiza la policía para cumplir su misión constitucional, por lo que resulta válido postular las siguientes tesis: primero, las operaciones psicológicas inciden en las operaciones policiales; y segundo, pueden emplearse en la lucha contra el crimen organizado y delincuencia común.

Desarrollo de las operaciones psicológicas

En la antigua China, las operaciones psicológicas se realizaron por primera vez, se caracterizaron por ser acciones destinadas a disuadir al enemigo, vencerlo o aparentar mayor fuerza frente a él. Este fenómeno alcanzó su máxima expresión con la divulgación de la obra "El arte de la guerra" de Sun Tzu (Tinoco, 2004). El personaje histórico de Sun Tzu fue un militar, estratega, escritor y filósofo chino, quien se enfocó en minar la moral del contrincante, rebajarlo y acabar con sus intenciones atemorizándolo, con el objetivo de triunfar sin recurrir al uso de las armas ni enfrentarse directamente al enemigo (Evans, 2005).

Las operaciones psicológicas, conocidas por sus siglas en inglés PSYOPs (Psychological Operations), se presentan como una de las herramientas más antiguas del arsenal humano. Se trata de un arma no letal capaz de neutralizar a los enemigos más feroces, moldear sus voluntades y creencias, y conocer sus debilidades y fortalezas (Chingo y Vásquez, 2018). El fundamento de las PSYOPs son la información y la comunicación que cumplen un rol determinante para influir en las actitudes de los individuos y alcanzar los objetivos de quienes las utilizan, para lo cual es imperante que estas operaciones estén integradas y coordinadas a través de planes estratégicos con todos los actores involucrados para maximizar la coherencia de los efectos psicológicos (NATO, 2012, 2014).

El propósito inicial de las operaciones psicológicas era evitar el conflicto y se consideraba una oportunidad para influir en el oponente. La victoria en un enfrentamiento no siempre se logra mediante la lucha directa, el uso de armas modernas o tecnología militar avanzada, sino también ganando en la mente de los individuos involucrados (Peña et al., 2009). Durante la Segunda Guerra Mundial, por ejemplo, estas operaciones se emplearon para penetrar en la psique del enemigo mediante el engaño y la creación deliberada de hechos ficticios, sembrando rumores y dudas entre sus filas (De Salvador, 2011).

En un sentido más amplio, las operaciones psicológicas se describen como acciones planificadas destinadas a suministrar información a objetivos específicos, como grupos, organizaciones o individuos, con el fin de influir en su pensamiento, emociones o razonamiento, lo que puede conducir a cambios en su comportamiento, ya sea para debilitarlo o fortalecerlo (Tinoco, 2005).

La literatura identifica cuatro características principales de las operaciones psicológicas, que incluyen corroer o debilitar la moral del enemigo, fomentar rendiciones

y deserciones, obstaculizar la difusión de propaganda y asegurar la colaboración de la población (Evans, 2005). Estas operaciones han sido y continúan siendo utilizadas como una herramienta en el ámbito militar. Se pueden mencionar casos de éxito, como la operación militar "Tormenta del Desierto", donde el uso planificado del engaño estimuló a la coalición, salvando numerosas vidas.

Operaciones psicológicas y tecnología

Las tecnologías de la información y comunicación (TIC) han coadyuvado a la difusión masiva de la información para captar la mente y corazón de las personas (Chingo y Vásquez, 2018), permitiendo que llegue en tiempo real y de una manera abrumadora a cualquier ciudadano, como a cualquier alto funcionario de una nación, lo que se convierte en un arma eficaz y potente (De Salvador, 2011).

Lo habitual, para lograr sus fines u objetivos es el uso de medios tangibles como las emisoras de radio, televisión, diarios, anuncios y cualquier otro medio que resulte capaz de influir en las personas con el gasto que ello acarrea, en la actualidad las redes sociales. No obstante, es evidente que las tecnologías de la información y comunicación, particularmente a través de medios digitales, son una alternativa real cuyo uso posibilita exponencialmente el éxito de las operaciones psicológicas.

Operaciones policiales

El trabajo policial en cualquier lugar del mundo resulta esencial, puesto que la labor del policía se enmarca en una serie de normas que limitan cualquier exceso. Esta situación es clave, puesto que es lo que diferencia a un Estado de Derecho de las dictaduras, siendo la normatividad en mención la que brinda las garantías a los ciudadanos frente a su actuación (Martínez, 2018). En el marco constitucional peruano, se establece que la Policía Nacional del Perú (PNP), tiene como finalidad fundamental:

> Garantizar, mantener y restablecer el orden interno. Presta protección y ayuda a las personas y a la comunidad. Garantiza el cumplimiento de las leyes y la seguridad del patrimonio público y del privado. Previene, investiga y combate la delincuencia. Vigila y controla las fronteras (Constitución Política Del Perú, 1993, Art. 166).

Por operaciones policiales se entienden todas aquellas acciones o actividades que realizan sus miembros en el ejercicio de su función para prevenir e investigar los delitos y faltas, así como todo lo relacionado a ello, identificando y estableciendo el grado de participación de los involucrados (Manual de Operaciones Policiales, 2013). El concepto de operaciones policiales es muy amplio y abarca un ámbito de acción complejo, sólo baste decir, que cada una de las Direcciones y Unidades y Subunidades Policiales de la PNP ejecutan operaciones policiales en el área de su responsabilidad.

En un concepto más restringido, las operaciones policiales representan un conjunto

de actividades planeadas, que son ejecutadas por unidades operativas del ente policial para cumplir con su finalidad fundamental, aplicando métodos y procedimientos establecidos en sus normas internas.

Operaciones psicológicas en la Policía Nacional del Perú

De la revisión de la literatura se advierte que el ejercicio de las operaciones psicológicas no se reduce a la práctica militar, en tiempo de paz o de guerra, sino que también, pueden usarse por el cuerpo policial. En la práctica se ha evidenciado que el uso de las operaciones psicológicas viene siendo utilizadas por la Dirección Contra el Terrorismo, así se establece en el reglamento de la Ley 1267, Ley de creación de la Policía Nacional del Perú, el cual precisa, entre otras funciones, el desarrollo de estrategias psicológicas en la lucha contraterrorista a nivel nacional (DS N° 026- IN, 2017).

La dirección emblemática de la institución policial cuenta con una División de Operaciones Psicológicas, la misma que se encarga de la realización de una serie de acciones estratégicas de índole ideológico, social y cultural para influir sobre determinado público neutral (población civil) y evitar de esta manera la captación ideológica por las huestes terroristas. Otro propósito, es lograr que los remanentes terroristas se desmoralicen y capitulen.

La realización de actividades cívicas, sensibilización de la población, apoyo social y otros que denotan la presencia del Estado por medio de la policía, coadyuvan al rechazo de organizaciones terroristas; en tal sentido y dando respuesta a la primera interrogante, se puede afirmar que las operaciones psicológicas inciden en las operaciones policiales; entendiendo a ésta última como la ejecución de operaciones destinadas a un combate frontal. Sin embargo, deben desarrollarse sutilmente con el apoyo de la tecnología, sin etiquetar la actividad como “operaciones psicológicas”, a fin de evitar cualquier cuestionamiento por parte de la opinión pública o ciudadanía en general, tal como ocurrió en Piura, en la que se denunció el uso de niños para dicho propósito (La República, 2023).

Si bien es evidente que las operaciones psicológicas son útiles en la lucha contraterrorista, se considera también, que lo propio puede resultar en la lucha contra la inseguridad ciudadana y el crimen organizado. Un ejemplo de su uso práctico se advirtió en la operación policial “Santa Anita”, donde por medio de la comunicación se expandió o propaló los rumores de desalojo, simulación de movimiento de personal policial, entre otras acciones psicológicas, lo que conllevó a mermar la moral de los invasores para luego ejecutarse las operaciones policiales con éxito según la Resolución Directoral N° 246-2013-DIRGEN/EMG del año 2013, este hecho develó su utilidad para la prevención de actividades delictivas.

Conclusión

Las operaciones psicológicas son actividades que primigeniamente fueron utilizadas

con éxito en el ámbito militar, que luego se extendieron al ámbito policial y político. Sobre los objetivos de las operaciones psicológicas, se orientan a influir/alterar el estado de ánimo de la población objetivo, así como mellar su moral, actitud y comportamiento, llamado oponente en el ámbito militar o la delincuencia en lo policial. Estas actividades se realizan mediante actividades sociales, culturales, acciones cívicas, así como con el uso de las tecnologías de la comunicación e información.

En las operaciones policiales, el uso de estas es previa y coadyuva al éxito de las operaciones policiales. Finalmente, el objetivo común es desmoralizar a los sujetos involucrados y debilitarlos para luego ejecutar las operaciones policiales planificadas, incrementando el éxito de las operaciones y/o intervenciones.

Referencias

Chingo, A., y Vásquez, E. (2018). Tecnología de la información y comunicaciónen las operaciones psicológicas en oficiales alumnos de escuela técnicadel ejército. Pensamiento Americano, 11(21), 229–236. https://dialnet.unirioja.es/servlet/articulo?codigo=8713916

Constitución Política del Perú (1993). https://www.congreso.gob.pe/Docs/files/documentos/constitucionpa rte1993-12-09-2017.pdf

De Salvador, L. (2011). Ingeniería social y operaciones psicológicas en internet. Instituto Español de Estudios Estratégicos, 1–21. https://www.ieee.es/Galerias/fichero/docs_opinion/2011/DIEEEO74-
2011.IngenieriaSocial_LuisdeSalvador.pdf

Department of Army (2003). Psychological Operations Tactics,Techniques, and Procedures. Field Manual FM 3-05.301 (FM 33-1-1). United States Department of the Army. https://irp.fas.org/doddir/army/fm3-05-301.pdf

Decreto Supremo N° 026-IN (2017). Reglamento del Decreto Legislativo No1267, Ley de la Policía Nacional del Perú. https://www.gacetajuridica.com.pe/boletin-nvnet/arweb/DS0262017IN.pdf

Evans, J. (2005). Uso y discurso de las operaciones psicológicas en los conflictos armados. II Congreso Internacional de Investigadores en Relaciones Públicas, Sevilla, España. https://idus.us.es/handle/11441/39274

La República (2023, 03 de febrero). Policías ejecutan operaciones psicológicas antiterroristas con niños de colegio de asentamiento humano. LR Norte. https://larepublica.pe/sociedad/2023/02/07/piura-policias-ejecutan-operacionespsicologicas-antiterroristas-ninos-de-colegio-de-asentamiento-humano-lrnd-482132

Martínez, R.(2018). La actuación policial en un contexto internacional: Algunas reflexiones sobre la IPTF y la policía de UNMIK. Anuario Español de Derecho Internacional, 17, 317–350. https://doi.org/10.15581/010.17.28464

North Atlantic Treaty Organization (2003). NATO Military Policy onPsychological Operations.

Document unclassified MC 402/1. NATO. https://info.publicintelligence.net/NATOPSYOPS-Policy-2003.pdf

North Atlantic Treaty Organization (2007). Allied joint doctrine for psychological operations. Document AJP -3.10.1(A). NATO. https://info.publicintelligence.net/NATOPSYOPS.pdf

North Atlantic Treaty Organization (2012). NATO Military Policy on psychological operations. Document unclassified MC 0402/02. NATO. https://info.publicintelligence.net/NATOPSYOPS-Policy.pdf

North Atlantic Treaty Organization (2014). Allied joint doctrine for psychological operations. Document AJP -3.10.1. Edition B Version 1. NATO. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attach ment_data/file/450521/20150223-AJP_3_10_1_PSYOPS_with_UK_Green_pages.pdf

Peña, L., Casas, L., y Mena, M. (2009). La Guerra Psicológica contemporánea conceptos esenciales y características. Humanidades Médicas, 9(2), 1–22. http://scielo.sld.cu/pdf/hmc/v9n2/hmc120209.pdf

Resolución Directoral No 246-2013-DIRGEN/EMG. (2013). Manual de operaciones sicológicas para la Policía Nacional del Perú. https://www.policia.gob.pe/Contenido/doc/docuDireasjur/MANUAL DE OPERACIONES PSICOLOGICAS DE LA PNP.pdf

Rodman, D. (2012). Perspectives of psychological operations (PSYOP) in contemporary conflicts: essays in winning hearts and minds. Israel Affairs, 18(4), 670-671. https://doi.org/10.1080/13537121.2012.718499

Tinoco, C. (2004). Dinámica del rumor y operaciones psicológicas de daño reputacional. Anales de La Universidad Metropolitana, 4(2), 155–169. https://dialnet.unirioja.es/servlet/articulo?codigo=4002584

Tinoco, C. (2005). Inestabilidad de la desinformación, escándalo y operaciones psicológicas. Anales de la Universidad Metropolitana, 5(1), 45–56. https://dialnet.unirioja.es/servlet/articulo?codigo=4001974

Vázquez, M. (1998). Las operaciones psicológicas y operaciones de informaciónde campaña. Boletín de Información, 255, 1-15. https://dialnet.unirioja.es/servlet/articulo?codigo=4643368

Vejvodová, P. (2019). Information and psychological operations as a challenge to security and defence. Vojenské rozhledy, 3, 83-96. https://www.ceeol.com/search/articledetail?id=797192

INICIP

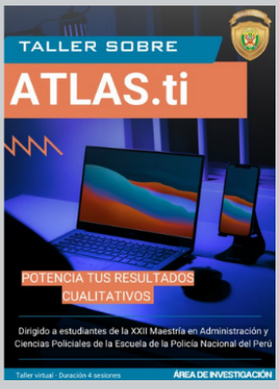
Instituto de investigación en Ciencias Policiales

Números publicados

Repositorio de tesis en RENATI

Capacitación

Cursos



ESCUELA DE POSGRADO

POLICIA NACIONAL DEL PERU

DIOS PATRIA LEY

Revista Académica Escpogra PNP
https://revistaescpograpnp.com/ojs/index.php/1/about
ISSN: 2961-2527 (En línea)

Revista Académica Escpogra PNP
https://revistaescpograpnp.com/ojs/index.php/1/about
ISSN: 2961-2527 (En línea)

Av. Guardia Civil N°800
La Campiña - Chorrillos
http://escpogra.pnp.edu.pe/portal/
Área de investigación de ESCPOGRA PNP