Jorge Isaac Cortez-Pepinos; Gladis Margot Proaño-Reyes; Gerardo Ramos-Serpa

<https://doi.org/10.35381/racji.v8i1.3454>

Autonomía y control de la Fiscalía General del Estado en el subsistema de interceptación de comunicaciones

Autonomy and control of the Attorney General's Office in the communications interception subsystem

Jorge Isaac Cortez-Pepinos

pg.jorgeicp94@uniandes.edu.ec

Universidad Regional Autónoma de Los Andes, Ambato, Tungurahua
Ecuador

<https://orcid.org/0009-0001-6209-1919>

Gladis Margot Proaño-Reyes

posgrado@uniandes.edu.ec

Universidad Regional Autónoma de Los Andes, Ambato, Tungurahua
Ecuador

<https://orcid.org/0000-0003-1653-5889>

Gerardo Ramos-Serpa

gerardoramos@uniandes.edu.ec

Universidad Regional Autónoma de Los Andes, Ambato, Tungurahua
Ecuador

<https://orcid.org/0000-0003-3172-555X>

Recibido: 15 de mayo 2023

Revisado: 20 junio 2023

Aprobado: 15 de agosto 2023

Publicado: 01 de septiembre 2023

Jorge Isaac Cortez-Pepinos; Gladis Margot Proaño-Reyes; Gerardo Ramos-Serpa

RESUMEN

El objetivo general de la investigación fue analizar jurídicamente la autonomía y control de la Fiscalía General del Estado en el subsistema de interceptación de comunicaciones. La presente investigación utilizó el método cuantitativo el cual produce datos descriptivos, que se originan por la recolección de datos. Apoyado en la revisión documental-bibliográfica. Además, se aplicó el método inductivo-deductivo. Se planteó además el método analítico-sintético. Se concluye que, El desarrollo y la penetración cada vez mayor de la tecnología se presenta con una gran cantidad de herramientas e instrumentos para las comunicaciones y para la interacción entre las personas, las cuales han hecho del uso de las aplicaciones tecnológicas tanto de su software como del hardware, verdaderos elementos de la cotidianidad, tanto para las cosas buenas y lícitas.

Descriptores: Tecnología; seguridad; protección de datos. (Tesauro UNESCO).

ABSTRACT

The general objective of the research was to legally analyze the autonomy and control of the Attorney General's Office in the subsystem of interception of communications. This research used the quantitative method which produces descriptive data, originating from data collection. Supported by the documentary-bibliographic review. In addition, the inductive-deductive method was applied. The analytical-synthetic method was also used. It is concluded that, the development and increasing penetration of technology is presented with a large number of tools and instruments for communications and for the interaction between people, which have made the use of technological applications of both software and hardware, real elements of everyday life, both for good and lawful things.

Descriptors: Technology; security; data protection. (UNESCO Thesaurus).

Jorge Isaac Cortez-Pepinos; Gladis Margot Proaño-Reyes; Gerardo Ramos-Serpa

INTRODUCCIÓN

Los avances tecnológicos representan una oportunidad para el desarrollo de la sociedad y el mejoramiento de las funciones que ejerce cualquier Estado. Producen también, incertidumbres en diferentes ámbitos de interés nacional, como la seguridad ciudadana y la defensa, con lo cual, los Estados promulgan leyes para regular la incidencia de estos medios tecnológicos para que contribuyan a la sociedad actual. Dicho de otra manera, según Lechner (2016), en cuanto a los avances tecnológicos, indica lo siguiente:

Las TIC's se complementan como herramientas para generar una reducción de incertidumbre y riesgo social, como una protección ante las amenazas. Esas certezas que generaban para dar confianza y protección tienen que estar en constante desarrollo y actualización, en concordancia con las mutaciones de los delitos y amenazas. (p. 3).

La innovación tecnológica, ha permitido la irrupción de nuevos medios de comunicación masivos que se desenvuelven en espacios de provecho para el Estado como el espectro radioeléctrico o el ciberespacio. El desarrollo de técnicas de vigilancia es consecuencia de los avances tecnológicos y un cambio de paradigma en su concepción (Osorio, 2018). La utilización de estos recursos, originan beneficios para la sociedad como: conocimiento, incentivos en producción y comercio, inclusión social, y otros. La telefonía móvil, por ejemplo, ha tenido la difusión más rápida y masiva de la historia de América Latina y el Caribe, así como en todo el mundo, lo que ha mejorado la calidad de vida de los segmentos más pobres de la población (Ayala y González, 2015).

Pese a eso, el crimen organizado suele también aprovecharse de este medio determinante de comunicación, estimulando el apareamiento de nuevos desafíos para la seguridad como el cibercrimen o la ciberdelincuencia, consideradas formas genéricas de las actividades ilícitas cometidas en el ciberespacio (Pons, 2017). Al contrario, el uso benéfico de herramientas tecnológicas con el fin de contrarrestar hechos punibles es una tendencia cada vez mayor en el mundo actual (Piracoca, 2016).

Jorge Isaac Cortez-Pepinos; Gladis Margot Proaño-Reyes; Gerardo Ramos-Serpa

De hecho, es tarea inquebrantable de los servicios de seguridad de cualquier nación, ocuparse de estos espacios, para propender a la convivencia social y pacífica de la población, promoviendo y protegiendo los derechos, garantías y libertades. En ese sentido, Casabianca (2015) indica lo siguiente:

La utilidad de las escuchas telefónicas como medio de investigación y fuente de prueba es indiscutible..., respetar y hacer viables garantías fundamentales de los ciudadanos investigados, dentro de las cuales se incluye el derecho al secreto de las comunicaciones... y acceso a la Justicia dentro de un debido proceso... (p. 343).

El periodista Ávila (2020) rememora los hechos ocurridos en relación con las interceptaciones ilegales por parte del DAS: recuerda que se hicieron famosas hace poco más de una década, cuando en el entonces gobierno de Álvaro Uribe se aprovechó del DAS, ocupándola como policía política para interceptaciones telefónicas, seguimientos ilegales a sindicalistas y académicos, y montajes contra la oposición. Posteriormente, el DAS fue disuelto por el gobierno de Santos. De igual forma, en julio de 2015, se hizo público información de la empresa italiana "*Hacking Team*".

En este sentido, Bonifaz y Delgado (2018) plantean lo siguiente:

Correos electrónicos, archivos digitales, códigos fuente, y otros, fueron expuestos en Internet. Según un informe realizado por la organización Chilena Derechos Digitales, Brasil, Chile, Colombia, Ecuador, Honduras, México y Panamá compraron licencias de software de esta empresa. Los países que compraron el software tienen legislación que limita el uso de este tipo de herramientas. (p. 324)

El Estado ecuatoriano tiene la atribución constitucional de desarrollar, ejecutar y coordinar planes y acciones para administrar la seguridad ciudadana, en tal virtud, en su planificación estratégica, se ha definido como amenaza o factor de riesgo a la agresión armada externa de actores no estatales, incidencia del crimen organizado transnacional, acciones terroristas con diversas motivaciones, flujo irregular de migrantes, acciones contra el Estado en el ciberespacio, degradación ambiental, ineficiencia estatal en prevención de delitos y violencia, y limitación en el desarrollo

Jorge Isaac Cortez-Pepinos; Gladis Margot Proaño-Reyes; Gerardo Ramos-Serpa

económico sostenido por presencia de flujos económicos ilícitos, entre otros temas afines.

En la presente investigación se plantea como objetivo general analizar jurídicamente la autonomía y control de la Fiscalía General del Estado en el subsistema de interceptación de comunicaciones.

MÉTODO

La presente investigación utiliza el método cuantitativo el cual produce datos descriptivos, que se originan por la recolección de datos. Apoyado en la revisión documental-bibliográfica. Además, se aplica el método inductivo-deductivo, el cual sugiere que para encontrar una verdad se deben buscar los hechos y no basarse en meras especulaciones, además de partir de afirmaciones generales para llegar a específicas (Dávila, 2006). Se plantea además el método analítico-sintético por medio del cual, se descompone un todo en partes extrayendo cualidades, componentes, relaciones y más para posteriormente unir las partes analizadas y con ello descubrir características y relaciones entre los elementos que son objeto de estudio (Rodríguez y Pérez, 2017).

RESULTADOS

De conformidad con la constitución y la legislación penal ecuatoriana, las comunicaciones protegen y garantizan el derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; ésta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen; este derecho protege cualquier otro tipo o forma de comunicación. Por lo que la interceptación de comunicaciones sin cumplir el debido proceso y realizada por la autoridad competente, podría constituir el delito de interceptación ilegal de datos, el cual se analiza en el siguiente cuadro conforme a lo establecido en el COIP (2018).

Jorge Isaac Cortez-Pepinos; Gladis Margot Proaño-Reyes; Gerardo Ramos-Serpa

Tabla 1.
 Análisis del delito de interceptación ilegal de datos.

Acción	Bien Jurídico Protegido	Sanción
1. Sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible. 2. Diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder. 3. A través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares. 4. Produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior.	La seguridad de los activos de los sistemas de información y comunicación	Pena privativa de libertad de 3 a 5 años.

Elaboración: Los autores.

Dado que la interceptación y demás acciones tendientes a hacerse del conocimiento de las informaciones y datos que son transmitidas por medios telefónicos e informáticos de cualquier tipo y alcance sin la autorización judicial correspondiente

Jorge Isaac Cortez-Pepinos; Gladis Margot Proaño-Reyes; Gerardo Ramos-Serpa

constituyen un delito sancionado con pena privativa de libertad, se precisa contar con reglas y normativas que establezcan disposiciones sobre la implementación, instalación, funcionamiento y control del organismo competente para la interceptación de comunicaciones o datos informáticos.

DISCUSIÓN

La interceptación de comunicaciones o datos informáticos que es autorizada por una autoridad judicial competente, y que es realizada por la FGE por medio del SICOM durante una investigación preprocesal o durante un proceso penal, debe ser entendida de forma estricta y limitada por los parámetros que la propia constitución y la legislación penal establecen, ya que interceptar, oír, grabar, entre otras acciones de las comunicaciones y los datos privados son una excepción a la seguridad y confianza que se prescriben como elementos esenciales de las comunicaciones por medios electrónicos. Lo que Baratta (2018) describe como la fusión y los beneficios del uso de la tecnología, entre los que se destacan la necesidad de reducción de la probabilidad de violaciones de privacidad, proporcionando mayor confianza en las interacciones con terceras personas.

Por otra parte, resulta pertinente acotar lo dicho por Núñez et al. (2019) con referencia al alcance de la implementación, instalación, funcionamiento y control de la interceptación de comunicaciones o datos informáticos, ya que, junto a los derechos fundamentales involucrados, como la intimidad, la inviolabilidad del domicilio o el secreto de las comunicaciones que se encuentran anotados en la sentencia del tribunal europeo, también resultará casi contraintuitivo dejar de investigar “todos” los delitos que surgen precisamente a partir de la investigación de otros delitos, y es aquí donde la FGE sería la llamada a atender tales cuestiones, por ser el organismo titular de la acción penal.

En este sentido, Borges (2018), sostiene que el uso de la prueba electrónica en el proceso penal, en particular la que puede ser obtenida mediante la interceptación de las comunicaciones o datos informáticos, presenta tanto ventajas como desventajas. Dentro de las ventajas se destaca que siempre y cuando el material no haya sido

Jorge Isaac Cortez-Pepinos; Gladis Margot Proaño-Reyes; Gerardo Ramos-Serpa

objeto de manipulación, estas pruebas ofrecen una información más objetiva, clara, precisa, completa y neutra que otros medios de prueba como pueden ser las declaraciones de testigos que siempre pueden contradecirse.

CONCLUSIONES

El desarrollo y la penetración cada vez mayor de la tecnología se presenta con una gran cantidad de herramientas e instrumentos para las comunicaciones y para la interacción entre las personas, las cuales han hecho del uso de las aplicaciones tecnológicas tanto de su software como del hardware, verdaderos elementos de la cotidianidad, tanto para las cosas buenas y lícitas, como son los emprendimientos, la educación a distancia, el comercio virtual, por mencionar algunos sectores informatizados con gran éxito, a lo que se adiciona el empleo de la tecnología para la investigación con fines de determinación y detección del delito.

FINANCIAMIENTO

No monetario.

AGRADECIMIENTO

A la Universidad Regional Autónoma de los Andes, por motivar el desarrollo de la Investigación.

REFERENCIAS CONSULTADAS

Asamblea Nacional (2014). Código Orgánico Integral Penal. [Comprehensive Criminal Code]. Registro Oficial N° 180. <https://url2.cl/53c6h>

Asamblea Nacional Constituyente de la República del Ecuador (2008). Constitución de la República del Ecuador. [Constitution of the Republic of Ecuador]. Montecristi. Registro Oficial 449 de 20-oct-2008. <https://n9.cl/i1ch>

Ávila, A. (13 de enero de 2020). Las interceptaciones ilegales en Colombia. [Illegal interceptions in Colombia]. Diario El País. <https://n9.cl/8kso7>

Jorge Isaac Cortez-Pepinos; Gladis Margot Proaño-Reyes; Gerardo Ramos-Serpa

- Ayala E. y González S. (2015). Tecnologías de la Información y la Comunicación. [Information and Communication Technologies]. Universidad Inca Garcilaso de la Vega. Lima Perú. <https://n9.cl/wd7zq>
- Baratta, R. (2018). Gobierno de la ciberseguridad. [Cybersecurity governance]. *Economía industrial*, 410, 61-70. <https://n9.cl/li40o>
- Bonifaz, R., y Delgado A. (2018). Casos verificados de uso ilegítimo de software de vigilancia por parte de gobiernos de América Latina. *Revista PUCE*, 106, 315-333. <https://n9.cl/lj6ry>
- Borges, R. (2018). La prueba electrónica en el proceso penal y el valor probatorio de conversaciones mantenidas utilizando programas de mensajería instantánea. [Electronic evidence in criminal proceedings and the probative value of conversations held using instant messaging programs]. *Revista Boliviana de Derecho*, 25, 536-549. <https://n9.cl/gwznc>
- Casabianca, P. (2015). Las Intervenciones Telefónicas en el Sistema Penal. [Wiretapping in the Penal System]. Tesis Doctoral. Universidad de Salamanca, España.
- Dávila Newman, G. (2006). El razonamiento inductivo y deductivo dentro del proceso investigativo en ciencias experimentales y sociales. [Inductive and deductive reasoning within the research process in experimental and social sciences]. *Laurus*, 12(Ext), 180-205. <https://n9.cl/nx847>
- Lechner, M. (2016). Tecnologías aplicadas a la seguridad ciudadana: desafíos para la justicia transicional ante nuevos mecanismos de control social. [Technologies applied to citizen security: challenges for transitional justice in the face of new mechanisms of social control]. *Divulgatio. Perfiles académicos de posgrado*. <https://n9.cl/px4tp>
- Núñez, R., Beltrán, R., y Santander, N. (2019). Los hallazgos casuales en las diligencias de incautación e intervención de las comunicaciones digitales en Chile. Algunos problemas. [The casual findings in the seizure and interception of digital communications in Chile. Some problems]. *Política Criminal: Revista Electrónica Semestral de Políticas Públicas en Materias Penales*, 14(28), 152-185. <https://n9.cl/6h2st>
- Osorio, C. (2018). Derecho a la privacidad y vigilancia masiva. [Right to privacy and mass surveillance]. Tesis de Grado. Universidad de Chile. <https://n9.cl/mobtin>

Jorge Isaac Cortez-Pepinos; Gladis Margot Proaño-Reyes; Gerardo Ramos-Serpa

- Piracoca, H. (2016). Evaluación de la regulación y de las herramientas tecnológicas de interceptación telefónica y su impacto a la seguridad nacional en Colombia. [Evaluation of the regulation and technological tools for telephone interception and their impact on national security in Colombia]. Tesis de Maestría. Universidad Nacional de Colombia. <https://n9.cl/hk5jw>
- Pons, V. (2017). Internet, la nueva era del delito: cibercrimo, ciberterrorismo, legislación y ciberseguridad. [Internet, the new era of crime: cybercrime, cyberterrorism, legislation and cybersecurity. Latin American Journal of Security Studies]. *Revista Latinoamericana de Estudios de Seguridad*, 20, 80-93. <https://n9.cl/djzb8l>
- Rodríguez, A., y Pérez, A. O. (2017). Métodos científicos de indagación y de construcción del conocimiento. [Scientific methods of inquiry and knowledge construction]. *Revista EAN*, 82, 179-200. <https://doi.org/10.21158/01208160.n82.2017.1647>