DERECHO A LA PRIVACIDAD Y OPERACIONES DE INTELIGENCIA EN ECUADOR

THE RIGHT TO PRIVACY AND INTELLIGENCE OPERATIONS IN ECUADOR

DIREITO A PRIVACIDADE E OPERAÇÕES DE INTELIGÊNCIA NO EQUADOR

*Martín Tamayo**

Recibido: 29/08/2020
Aprobado: 26/10/2020

Resumen

Las tensiones entre el derecho a la privacidad y la intercepción de comunicaciones digitales durante operaciones de inteligencia se reflejan en la Ley de Seguridad Pública y del Estado del Ecuador. El objetivo es determinar si esta regulación de 2009 respeta el derecho a la privacidad en la era digital, como una expresión de la dignidad humana. El estudio fue realizado en base a un análisis comparativo de autores, legislación e informes de derechos humanos. No existen medios efectivos para asegurar que el Estado ecuatoriano no vulnere ilegalmente la privacidad durante operaciones de vigilancia, en irrespeto a la Constitución, estándares interamericanos y universales. La ambigüedad en la justificación de las interceptaciones menoscaba una visión de seguridad integral y vulnera derechos.

Palabras clave: Derechos Humanos; Dignidad; Era Digital; Intercepción; Privacidad; Seguridad Integral; Vigilancia

Abstract

The tensions between the right to privacy and the interception of digital communications, during intelligence operations, are reflected in the Public and State Security Act of Ecuador. The objective of this paper is to understand if this regulation (issued in 2009) respects the right to privacy in the digital age, as an expression of human dignity. The study was conducted through a comparative analysis of authors, legislation, and human rights reports. No effective means to ensure that the Ecuadorian State does not illegally violate the right to privacy during surveillance operations are available, disrespecting Constitutional, Inter-American, and universal standards. Ambiguity in the justification of surveillance undermines an integral security vision and undermines human rights.

Key words: Digital Age; Dignity; Human Rights; Integral Security; Interception; Privacy; Surveillance

Resumo

As tensões entre o direito à privacidade e a interceptação de comunicações digitais durante operações de inteligência se refletem na Lei de Segurança Pública e do Estado do Equador. O objetivo é determinar se esta regulação de 2009 respeita o direito à privacidade na era digital, como uma expressão da dignidade humana. O estudo foi realizado baseado numa análise comparado de autores, legislação e informes de direitos humanos. Não existem meios efetivos que assegurem que o Estado equatoriano não lesione ilegalmente a privacidade durante operações de vigilância o que ocasiona uma violação a Constituição, padrões interamericanos e universais. A ambiguidade na justificação das interceptações afeta uma visão de segurança integral e vulnera direitos.

Palavras chave: Direitos Humanos; Dignidade; Era Digital; Interceptação; Privacidade; Segurança Integral; Vigilância

* Máster en Derecho (LL.M) con mención en Derecho Internacional Público, por The London School of Economics and Political Science; Especialista Superior en Derechos Humanos, por la Universidad Andina Simón Bolívar; Abogado por la Universidad San Francisco de Quito. Funcionario del Ministerio de Relaciones Exteriores y Movilidad Humana del Ecuador, especializado en derechos humanos y seguridad internacional. Correo electrónico: martintamayo1@gmail.com

There is, simply, no way, to ignore privacy. Because a citizency's freedoms are interdependent, to surrender your own privacy is really to surrender everyone's.

Edward Snowden, 2019
Permanent Record

INTRODUCCIÓN

El estudio examina la tensión entre la privacidad y la forma de regular las operaciones de inteligencia en el Ecuador. La relación entre el derecho a la privacidad sobre la información personal y la normativa que rige la intercepción de telecomunicaciones, en operaciones de inteligencia, es estudiada a la luz de la Ley de Seguridad Pública y del Estado (LSPE) vigente desde 2009.

En este trabajo, el derecho a la privacidad y la inviolabilidad de las comunicaciones son abordados como una expresión de la dignidad humana. Según Post (2001) y Whitman (2004), la vulneración de la privacidad no solo constituye una violación a la autonomía personal -considerada como una forma de autodeterminación respecto a la información propia y el control sobre esta- sino que supone una ofensa a la dignidad humana. Una transgresión atenta contra la visión colectiva de respeto personal, basada en principios intersubjetivos de convivencia. El respeto del derecho a la privacidad es una forma de defender un valor instrumental para el goce de otros derechos (Whitman 2004). Toda violación a este derecho constituye un atentado contra la sociedad y tiene una afectación particular en la dignidad individual (Corral 2000). La garantía de la privacidad contempla que cualquier vulneración, incluida la intercepción de comunicaciones, rompe las normas de convivencia en una sociedad democrática.

En este marco, cabe preguntarse cómo la privacidad de las personas podría ser vulnerada por la intercepción de telecomunicaciones, en operaciones de inteligencia, bajo la LSPE. El objetivo es determinar si la forma de regular la intercepción de comunicaciones en la LSPE, durante operaciones de inteligencia, atenta contra el derecho a la privacidad.

La privacidad es reconocida como un derecho humano que contempla el respeto irrestricto de la protección de las comunicaciones privadas. Las Constituciones del Ecuador, desde 1835 (Ávila 2012), así como instrumentos internacionales de derechos humanos, garantizan el secreto y la inviolabilidad de las comunicaciones (DUDH, art. 12; CADH, 1969; art. 11.2; art. 17). Estos aspectos garantizan el ejercicio del derecho a la privacidad y están vinculados con la dignidad humana (Escalante 2004). Mediante la aplicación del principio de progresividad y frente al desarrollo digital, este derecho es extensible a toda forma de comunicación privada (Ávila 2009).

El Estado tiene la capacidad de restringir el derecho a la privacidad y obtener información personal que califica como inteligencia. Según la Constitución, este derecho puede ser limitado por una ley (CE, Art. 66). La LSPE (art. 20) establece una restricción a la inviolabilidad del secreto de correspondencia, mediante un proceso judicial, para obtener información de inteligencia (LSPE, art. 4). No obstante, estos aspectos de la LSPE han sido criticados por atentar contra el debido proceso, la intimidad personal y la inviolabilidad de la correspondencia (Hurtado 2010, 107). Los organismos vinculados con la intercepción de comunicaciones, como la Secretaría de Inteligencia (SIN), ahora Centro de Inteligencia Estratégica (CIES) (DE 536, art. 4), y los órganos que administran justicia, tienen la obligación de velar por el respeto de la privacidad en los procesos (LSPE, art. 20).

En los últimos años, el debate entre privacidad y vigilancia fue revitalizado. Edward Snowden reveló un sistema de espionaje masivo indiscriminado de Estados Unidos a nivel global (Greenwald 2014). Hacking Team, especializada en herramientas de espionaje

electrónico, fue vinculada a la firma Robotec, que a su vez era proveedora de la SIN (Ricaurte 2015). Desde el 2016, los atentados del autoproclamado Estado Islámico en Europa renovaron el discurso restrictivo de libertades, incluida la privacidad, frente a la protección de la seguridad nacional (Bigo et al 2015; CDHNU 2018).

En su informe de 2018, el relator especial sobre la intimidad, Joseph Cannataci, no encontró ninguna legislación nacional sobre vigilancia que cumpla con los estándares internacionales que protegen ese derecho (CDHNU 2018). Este contexto justifica la necesidad de un estudio crítico sobre la relación entre privacidad y actividades de vigilancia en el Ecuador.

El impacto de la LSPE es analizado desde su promulgación en 2009, con énfasis en las políticas públicas de seguridad emitidas desde por el Gobierno desde el 2017, incluidas algunas que tienen una aspiración de regir hasta el año 2030. En el presente trabajo se incorporan los aportes de Freddy Rivera y Katalina Barreiro (2011; 2017) relativos a la producción académica sobre inteligencia en el Ecuador. Las justificaciones para interceptar comunicaciones implican una interpretación de la inteligencia como una herramienta de seguridad nacional (Rivera et al 2011). Las justificaciones maleables de seguridad para obtener inteligencia generan potenciales desvíos corporativos susceptibles de politización (Rivera 2017). Las publicaciones académicas e informes de derechos humanos sobre el alcance de la privacidad se examinan en su relación con operaciones de órganos de seguridad e intercepción de comunicaciones. Y la legislación, las políticas públicas, los instrumentos internacionales, así como estándares de los sistemas interamericano y universal de derechos humanos se estudian respecto a la intercepción de telecomunicaciones.

INTERCEPCIÓN DE TELECOMUNICACIONES Y ELEMENTOS ESENCIALES DEL DERECHO A LA PRIVACIDAD

En primer lugar, la LSPE desarrolla la regulación de la intercepción de las comunicaciones para obtener información vinculada a inteligencia. El procedimiento legal y las garantías para las personas sujetas a estas intervenciones muestran deficiencias que restringen el derecho a la privacidad. Además, la justificación de la intercepción de comunicaciones podría contraponerse con la concepción de seguridad integral, que implica un riesgo de politización y abusos.

En esta medida, los elementos esenciales de este derecho, desde una visión de protección de la dignidad humana, son identificados para determinar si el nivel de acceso y de control del Estado constituyen una intromisión ilegítima y arbitraria que menoscaba este derecho.

Regulación de la intercepción de comunicaciones en el Ecuador

En el Ecuador, la Constitución garantiza el derecho a la privacidad a través de la protección de las comunicaciones, y contempla una excepción para romper el secreto de la correspondencia mediante una ley (CE, art. 66.21). La LSPE regula el procedimiento para la intercepción de comunicaciones durante operaciones de inteligencia. El artículo 20 dictamina que, en operaciones encubiertas, si los organismos de inteligencia requieren una intercepción, deben solicitar una autorización judicial reservada que no afecte los derechos de las personas involucradas y que carezca de cualquier beneficio político (LSPE, art. 20).

En este trabajo, solo se analiza la intercepción de comunicaciones del sistema nacional de inteligencia. Este procedimiento no se aplica a las etapas pre-procesales y procesales de la fiscalía general del Estado o el subsistema de inteligencia antidelincuencial de la policía nacional (COESCOP, art. 69) para resolver la comisión de delitos. El Código Orgánico Integral Penal (COIP) contempla un apartado particular sobre actuaciones especiales de investigación, que regula las indagaciones e incluye la intercepción de comunicaciones en juicios penales (COIP, art. 475).

La LSPE dispone la eliminación de la información si los datos recolectados no permiten iniciar una acción penal. Las grabaciones y los documentos deben ser destruidos con autorización y ante un juez. La LSPE remite a su reglamento para establecer un procedimiento de modo que la persona objeto de la investigación sea notificada, como requisito previo a la destrucción de la información (LSPE, art. 20). El reglamento no menciona este procedimiento (Reglamento LSPE). En la aprobación de la intercepción, los jueces deben orientar las acciones de las autoridades hacia el respeto de los derechos humanos (LSPE, art. 20).

La intercepción de telecomunicaciones se justifica como medio para obtener información de inteligencia expresamente vinculada con la protección de la seguridad integral (LSPE, art. 20).

Valoración positiva de la concepción normativa del derecho a la privacidad

La contraposición de intereses entre el respeto del derecho a la privacidad y la intercepción de telecomunicaciones con fines de inteligencia es estudiada desde las categorías de análisis de Helen Nissenbaum (2010) en el establecimiento del valor de la privacidad. En concordancia con Post y Whitman (2004), una concepción normativa de la privacidad no es neutral, sino que aporta un elemento valorativo positivo sobre la necesidad de proteger la privacidad, desde un punto de vista individual y colectivo. En efecto, la relevancia normativa de la privacidad supone que su utilidad está vinculada con la necesidad de una reglamentación que limite cualquier vulneración a la información privada. Por lo tanto, su protección debe garantizarse por medios estatales efectivos de amparo (Nissenbaum 2010).

En la línea de pensamiento de Nissenbaum, para comprender la problemática de la intercepción de comunicaciones, la privacidad es un derecho influenciado por el concepto de control. En efecto, autores como Michael Froomkin describen a este derecho como "la capacidad de controlar el acceso o difusión de la información sobre uno mismo" (2000, 1164). La privacidad no solo está marcada por la restricción del acceso a datos por parte de terceros, sino por el control que los individuos y la sociedad tienen sobre la circulación de información privada (Nissenbaum 2010). Una negociación continua sobre el control de los datos se desarrolla entre el individuo y la sociedad, con el Estado como intermediario, para determinar el grado adecuado de acceso a la información que garantice el derecho a la privacidad, frente a intereses colectivos, en una sociedad democrática. A continuación, se analiza la compatibilidad de una visión de seguridad nacional, disfrazada bajo seguridad integral, con la regulación de operaciones de inteligencia, ante su potencial politización.

Aparente centralidad de los derechos, incluida la privacidad, en las políticas públicas de seguridad

A primera vista, la LPSE se alejaría de una visión de seguridad nacional y se acercaría a una política de seguridad integral alineada con la Constitución (2008, art. 85 y 393). Antes de la LSPE, estaba vigente la Ley de Seguridad Nacional de 1960, influenciada por las políticas de seguridad hemisféricas, orientada a proteger la integridad del Estado y la paz social (Rivera 2012). Según la LSPE (art. 20), la preservación de la seguridad coadyuva al ejercicio de derechos.

Esta visión que transversaliza una perspectiva de derechos en las políticas de seguridad ha sido reforzada desde el 2017 (Plan Nacional de Desarrollo, 56). El Plan Nacional de Seguridad Ciudadana y Convivencia Social Pacífica contempla que "la seguridad ciudadana (…) toma al enfoque de derechos humanos para profundizar la efectiva gobernabilidad de las instituciones" (2019, 32). El Plan Específico de Inteligencia (2019) orienta al sistema nacional de inteligencia hacia la protección de la seguridad integral. El objetivo de la seguridad integral es el respeto de los derechos humanos en todo contexto, incluidas las actividades orientadas a proteger la misma seguridad (Benavides y Chávez 2013). Este enfoque no buscaría preservar la integridad del Estado y la paz social, como un fin en sí mismo. Sin embargo, para el Plan Nacional de Seguridad Integral, que cobija las demás políticas sectoriales, el sistema nacional de inteligencia tiene por objetivo la generación de información sobre riesgos y amenazas "para la defensa y seguridad pública del Estado" (2019, 108). Este sería un retorno a doctrinas

de seguridad nacional identificadas por Rivera (2017), que sobredimensionan el rol de los Estados sobre la sociedad, sin una perspectiva de derechos. La Política de la Defensa Nacional ratifica este retroceso con un rol omnipresente de las Fuerzas Armadas y una vocación de "tutelaje militar sobre seguridad interior y desplazando el control civil" (Rivera 2019, 25-26). La seguridad del Estado se traduce en la protección de la gobernabilidad democrática, aunque en realidad vela por la estabilidad del Gobierno en el poder. La ambigüedad en la definición de las amenazas a la seguridad, el rol ubicuo autoasignado a los subsistemas de inteligencia, además de la falta de una planificación coherente (Rivera 2019) generan una multiplicidad de justificaciones infundadas para la activación de los subsistemas de inteligencia.

El derecho a la privacidad puede ser vulnerado por una maleable concepción de seguridad que faculta a una inteligencia con fines políticos. En efecto, María Ordóñez y Galo Cruz (2017) estiman que el sistema nacional de inteligencia pudo haber sido orientado para prácticas partidistas que distorsionan sus objetivos, "restringido a lo establecido en agendas políticas" y sujeto a actos discrecionales. La ambigüedad de los objetivos del sistema nacional de inteligencia y el regreso en la práctica a una concepción de seguridad nacional tradicional facilitarían una politización de las operaciones de intercepción de comunicaciones y restricciones arbitrarias a la privacidad.

El riesgo de politización de los sistemas de inteligencia es magnificado por garantías normativas y estructurales deficientes que no alinean la intercepción de las comunicaciones con estándares de derechos humanos, como se describe a continuación. En este contexto, la compatibilidad y coherencia de los elementos constitutivos del derecho a la privacidad serán contrastados con su restricción en la LSPE.

Elementos esenciales del derecho a la privacidad, como una expresión de la dignidad humana, frente a la regulación de las operaciones de inteligencia

El preámbulo de la Constitución (2008) orienta la construcción de una sociedad que respete la dignidad de las personas en un sistema democrático. Estos valores tienen un efecto de emanación sobre el ordenamiento jurídico nacional y el poder público (Trujillo 2013, 108). La LSPE debe respetar la dignidad humana, en una sociedad democrática, traducida en la protección del derecho a la privacidad.

El derecho a la privacidad genera una obligación de protección de las comunicaciones y de la intimidad personal. La Constitución garantiza el derecho a la protección e inviolabilidad de la correspondencia, inclusive por medios digitales (CE art. 66.21). El sistema legal debe imponer severos límites a la vulneración de la privacidad, por su vinculación con otros derechos y el valor normativo individual y social que se asigna a inviolabilidad de la intimidad personal (Nissenbaum 2010).

En Ecuador, el derecho a la privacidad está marcado por el control sobre la información personal. La privacidad está delimitada por la amplitud o restricción de la difusión de la información personal frente a terceros y su circulación en la sociedad (Froomkin 2000). El ordenamiento de la intercepción de telecomunicaciones supone un dilema sobre la potestad del Estado para intervenir en el control de la información. Los derechos son ponderados en relación con los intereses colectivos, a través de la obtención de inteligencia para preservar la seguridad integral.

Una forma de control de la información en la LSPE corresponde a la destrucción de la información recolectada con fines de inteligencia. Previamente a su eliminación, la persona intervenida debe ser notificada si sus comunicaciones recolectadas no establecieron una responsabilidad penal. La LSPE establece que su reglamento debe desarrollar un procedimiento de notificación para conocer la información recabada antes de su destrucción (LSPE, art. 20). El reglamento no especifica este proceso. Esta laguna legal imposibilita que una persona que haya sido investigada de forma infundada o abusiva pueda conocer la existencia de una vulneración a sus derechos. Si no existe un proceso para notificar a la víctima y la información fue destruida, la persona que sufrió una vulneración a su privacidad no puede ejercer su derecho a la tutela judicial efectiva y el acceso a la justicia, en vista de

que las pruebas de la intercepción fueron eliminadas (Hurtado 2010).

En relación con el control sobre la información desde el Estado, la LSPE no contempla otros escenarios para prevenir o reparar la vulneración de los derechos de terceras personas. La intercepción versa sobre comunicaciones interpersonales. Razón por la cual, no solo existiría una vulneración sobre la persona investigada, sino una violación de la privacidad de aquellos individuos con quienes la persona investigada mantenía comunicaciones.

De la misma forma, en la LSPE no se contempla una vulneración de derechos por la excesiva recolección de información no vinculada con los fines de la investigación. Los avances en las tecnologías de la información de seguridad alcanzan métodos de vigilancia más intrusivos y continuos sobre la información personal (Nieves 2007). Una investigación requiere un acceso constante, durante un amplio periodo de tiempo -hasta 120 días- sobre las comunicaciones de una persona (LSPE, art. 20). Sin embargo, la LSPE no establece una forma de rendición de cuentas sobre la información individual recolectada extensivamente pero que no está asociada con el propósito de la investigación.

La LSPE establece una prohibición para la producción de inteligencia sobre personas por motivos de "etnia, orientación sexual, credo religioso, acciones privadas, posición política" (LSPE, art. 21-22) o pertenencia a algún partido o movimiento social. Esta prohibición, al omitir categorías sobre igualdad y no discriminación de la Constitución (art. 11.2), reafirma la falta de un enfoque de derechos en la intercepción de comunicaciones.

Así mismo, el artículo 20 de la LSPE sobre la acción de los jueces ante solicitudes de intercepción admite interpretaciones que podrían vulnerar derechos. El juez puede negar una solicitud de intercepción "por afectación grave a los derechos de los sujetos sobre quienes se ejerce la operación encubierta" (LSPE, art. 20). Esta formulación es problemática. ¿Podría un juez autorizar una intervención de organismos de inteligencia si existe solo una "leve" afectación a los derechos? Se trata de una doctrina no reconocida hasta el momento. Las únicas vulneraciones que justificarían negar una intercepción serían las graves violaciones a los derechos humanos. Estas son reconocidas como tales por el derecho internacional o por el capítulo I del título IV del COIP, como los delitos de lesa humanidad, crímenes de guerra, etnocidio, ejecuciones extrajudiciales, entre otras (COIP, arts. 79-90). Así, el uso del adjetivo "grave" en el artículo 20 de la LSPE abre un espacio de subjetividad que no garantiza la protección de derechos.

De tal manera que, varias disposiciones que regulan la intervención en comunicaciones contravienen los elementos centrales del derecho a la privacidad. Este garantiza la inviolabilidad y el secreto de la correspondencia, como una forma de proteger el control sobre el nivel de difusión de la información personal y familiar. En dicho marco, la LSPE no solo debe adecuarse a la Constitución, sino a los instrumentos internacionales de derechos humanos. En el siguiente acápite se analizan, los estándares del sistema interamericano y universal de derechos humanos frente a las disposiciones de la LSPE relativas a inteligencia e intercepción de comunicaciones. Estos estándares esclarecen el alcance de las obligaciones estatales relativas al derecho a la privacidad, en la era de las nuevas tecnologías de la información y comunicación.

INTERCEPCIÓN DE TELECOMUNICACIONES EN OPERACIONES DE INTELIGENCIA A LA LUZ DEL DERECHO INTERNACIONAL DE LOS DERECHOS HUMANOS

Las opiniones de los órganos especializados en la promoción y la protección de derechos humanos ayudan a comprender las obligaciones de los Estados respecto al derecho a la privacidad en actividades de inteligencia. Los estándares de los sistemas interamericano y universal desarrollan el alcance de las obligaciones para el Ecuador. Estos organismos analizan como compatibilizar la intercepción de comunicaciones con

la protección y garantía de derechos, en un Estado democrático.

Estándares del sistema interamericano sobre limitaciones al derecho a la privacidad

Por un lado, la Convención Americana sobre Derechos Humanos (CADH), ratificada por el Ecuador en 1977, garantiza el derecho a la vida privada. Con relación a la protección de la dignidad, establece que "[n]adie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia" (CADH, art. 11.2). Esta garantía ratifica la inviolabilidad y secreto de la correspondencia garantizada en la Constitución y enfatiza la prohibición de injerencias en la vida privada.

Por otro lado, la jurisprudencia de la Corte Interamericana de Derechos Humanos (CorteIDH) ha determinado el alcance del derecho a la vida privada. El caso Tristán Donoso vs. Panamá reconoció que "el ámbito de la privacidad se caracteriza por quedar exento e inmune a las invasiones o agresiones abusivas o arbitrarias de terceros o de la autoridad pública" (CorteIDH 2009, 55). La Corte extendió el artículo 11 de la CADH a cualquier tipo de comunicación, incluso aquellas no contempladas expresamente, razón por la cual incluye escenarios de la era digital (Ávila 2009). Sin embargo, el derecho a la privacidad puede ser restringido.

En el 2009, la Comisión Interamericana de Derechos Humanos (CIDH) emitió un informe sobre seguridad ciudadana y derechos humanos. El documento establece condiciones, en contextos excepcionales, para restringir la privacidad. Las limitaciones a la privacidad solo deberían enfocarse en las acciones del poder público para prevenir y sancionar hechos delictivos, como un medio para el asegurar la consecución de investigaciones judiciales (CIDH 2009).

En el Ecuador, dos cuerpos normativos permiten interceptar comunicaciones. Por una parte, el COIP (2014) contiene un capítulo para la intercepción de comunicaciones durante actuaciones especiales de investigación de la comisión de delitos (art. 475). Esta limitación a la privacidad, con fines judiciales de persecución de delitos, guardaría conformidad formal con los lineamientos establecidos por la CIDH.

Por otra parte, la LSPE no establece que la finalidad de la intercepción de comunicaciones sea únicamente la persecución de delitos, pues no restringe el derecho a la vida privada únicamente para investigarlos, sino también para otros fines de inteligencia (LSPE, art. 14.a), cuya amplitud no está definida y puede ser maleable, como fuera observado con anterioridad. Además, la LSPE podría infringir los estándares de la CIDH si no incorpora las garantías apropiadas.

El procedimiento de la LSPE debe ser coherente con los derechos vinculados al debido proceso; por ejemplo, a la observancia de los artículos 8 y 25 de la CADH sobre garantías procesales y protección judicial. La Constitución plasma la aplicación directa de los instrumentos internacionales más favorables para asegurar la vigencia de los derechos (CE, art. 424). La CADH y las decisiones de los órganos del sistema interamericano constituyen un referente para analizar el derecho a la privacidad.

Una regulación de la vigilancia de comunicaciones privadas como la establecida en la LSPE debe ser clara con el objeto de garantizar el respeto del debido proceso, un equilibrio entre las partes y evitar abusos. La jurisprudencia de la CorteIDH, cuya interpretación esclarece el alcance de la CADH, establece que el derecho al debido proceso implica "un justo equilibrio entre el ciudadano y el Estado, donde las garantías procesales adquieran sentido y actualidad al evitar la arbitrariedad e inseguridad" (Rodríguez 1998, 1297).

Tal como se indicó en el anterior acápite, en la LSPE existe un desequilibrio procesal por la imposibilidad de que una persona que haya sido investigada sin fundamento pueda conocer la existencia de una dicha vulneración. El reglamento de la LSPE no establece el procedimiento para incorporar en el proceso a una presunta víctima. Sin un procedimiento para notificar y dar a conocer las piezas procesales producidas durante una intervención por inteligencia, el acceso a la justicia no está garantizado ante una vulneración del derecho a la privacidad.

Sobre el principio de responsabilidad estatal, en el sistema interamericano, Tara Melish identifica principalmente las obligaciones de respeto y garantía de los derechos para los Estados. El deber de respeto implica una abstención de realizar conductas atentatorias contra los derechos. La garantía es una obligación positiva de "organizar todas las estructuras […] del poder público de manera tal que sean capaces de asegurar jurídicamente el libre y pleno ejercicio de los derechos humanos" (Melish 2003, 175-177). Así, la LSPE debería contemplar mecanismos efectivos para la vigencia de los derechos en la intercepción de comunicaciones. Si bien prohíbe el uso de la inteligencia para fines políticos o personales (LSPE, art. 20), no establece un procedimiento sancionador del uso inadecuado de los mecanismos de intercepción. Tampoco incorpora medios para una posible reparación de las víctimas de una vulneración.

En principio, la acción de protección (CE, art. 88) es una garantía judicial de amparo que podría ser activada. En el presente caso, un juez podría declarar la vulneración de un derecho constitucional y la reparación a la víctima. Los estándares interamericanos detallan que "la función de esos recursos […] sea idónea para proteger la situación jurídica infringida [...] además, eficaz, es decir, capaz de producir el resultado para el que ha sido concebido" (CorteIDH, Velásquez Rodríguez vs. Honduras, 64-68). En la situación bajo estudio, no existe un medio efectivo de reparación de una violación del derecho a la privacidad en el caso de que las evidencias sean destruidas, sin una notificación de esta circunstancia a la posible víctima. Así, este recurso judicial no cumple con los estándares interamericanos sobre acceso a la justicia para el derecho a la privacidad.

Por otro lado, la CIDH contempla que las restricciones al derecho a la vida privada deben estar "justificadas en la necesidad de proteger los derechos de terceras personas y el interés general de la sociedad" (CIDH 2009, 175). Según el artículo 30 de la CADH (1969), los derechos pueden ser restringidos únicamente mediante una ley justificada por el interés general. La CorteIDH estableció el alcance de la palabra "leyes". Estas deben ser emitidas de manera formal y material; y, cualquier restricción debe apegarse al bien común, en un Estado democrático (CorteIDH 1986). En el Ecuador, el bien común y el interés general que justifican la restricción de la privacidad corresponden a la identificación de información que garantice la seguridad integral (LSPE, art. 4).

Como fuera observado en la revisión de las políticas públicas de seguridad y la LSPE, el enfoque de seguridad nacional para la preservación de la integridad del Estado permanece fortalecido. El Estado debe velar por el respeto del derecho a la privacidad, por encima del interés general o el bien común, durante las operaciones de inteligencia (Ávila 2009). En la LSPE, el Estado no alinea sus postulados con la garantía de la privacidad; porque privilegia la necesidad de resguardar al Estado (Rivera 2012), proteger el orden público y la convivencia (LSPE, art. 4), mientras que deja en un segundo plano los derechos humanos. La seguridad protegida por el sistema nacional de inteligencia contradiría los estándares interamericanos sobre restricciones permisibles al derecho a la vida privada. Las justificaciones de operaciones de inteligencia no velarían por el bien común en un estado democrático, sino por los intereses de la seguridad nacional, del orden público y del Gobierno. Lo peor es que estos, por su ambigüedad, pueden incluir el servicio a agendas políticas[1].

De esta manera, la regulación de la intercepción de comunicaciones en la LSPE contiene provisiones que no garantizan el derecho a la privacidad según los estándares del sistema interamericano de derechos humanos. Ahora, la regulación de la LSPE también debería guardar coherencia con los lineamientos establecidos por el sistema universal de protección de derechos.

Estándares del sistema universal sobre limitaciones al derecho a la privacidad

Varios instrumentos internacionales de Naciones Unidas garantizan el derecho a la privacidad. La

1 Artículo de Paul Mozur, Jonah Kessel y Melissa Chan, publicado en el New York Times, el 24 de abril de 2019: «Hecho en China y exportado a Ecuador: el aparato de vigilancia estatal». https://www.nytimes.com/es/2019/04/24/espanol/america-latina/ecuador-vigilancia-seguridad-china.html

Declaración Universal de Derechos Humanos contempla una prohibición de toda injerencia arbitraria en la vida privada, la correspondencia entre las personas y establece la necesidad de una protección de la ley frente a posibles abusos (DUDH, art. 12). Este derecho, y su correlativa garantía, fueron reafirmados por el Pacto Internacional de Derechos Civiles y Políticos (PIDCP, art. 17), ratificado por el Ecuador en 1968. La regulación de este derecho requiere herramientas adecuadas para enfrentar los retos emergentes del rápido desarrollo de las tecnologías, que permiten la vasta e indiscriminada recolección de datos en internet (Froomkin 2000).

El artículo 17 del PIDCP no desarrolla limitaciones explícitas para evitar vulneraciones a tal derecho, a diferencia de otros artículos de ese mismo tratado. En el año 2014, la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (OACDH) identificó que la principal afectación a la privacidad ocurre debido a la vigilancia masiva e intercepción de comunicaciones digitales de los Estados (CDHNU 2014,). El desarrollo de organismos de Naciones Unidas actualiza y adecua el alcance de los derechos a las nuevas tecnologías.

El sistema universal de derechos humanos establece estándares que desarrollan el contenido de las obligaciones estatales sobre el derecho a la privacidad. La Corte Constitucional reconoció al *soft law* con un valor jurídicamente relevante para interpretar el alcance del contenido de los derechos (CC, sentencia N.º 001-10-SIN-CC, 58). La Defensoría del Pueblo lo considera como una referencia de interpretación doctrinaria (2015). Estos estándares serán analizados en relación con la limitación a la privacidad en operaciones de inteligencia.

En el 2014, el Grupo de Trabajo sobre la protección de los derechos humanos en la lucha de la ONU contra el terrorismo estableció principios sobre el derecho a un juicio justo y el debido proceso en el combate al terrorismo. Según el principio 3 del documento, el derecho a un juicio justo implica la publicidad de los procesos. Cualquier restricción a este principio, incluso por motivos de seguridad nacional, debe ser necesaria, proporcional y analizada en función de cada caso (CTITF 2014). Estas restricciones deben ir acompañadas de mecanismos adecuados para garantizar un equilibrio procesal y una posible responsabilidad ulterior.

La LSPE no establece un análisis casuístico de la restricción a la publicidad del proceso. Con relación a la intercepción de comunicaciones, "[t]odas las actuaciones judiciales relativas a dicha solicitud mantendrán la reserva" (LSPE, art. 20). No existe una forma de vigilar la transparencia del procedimiento judicial y la eventual responsabilidad ante abusos de poder y violaciones de derechos. La LSPE no guardaría coherencia con el corpus iuris de los derechos humanos; como, por ej., con estos principios de Naciones Unidas sobre la necesidad de publicidad en el control de operaciones de inteligencia.

De la misma forma, el relator especial sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, en su informe del 2014, reiteró la necesidad de medios efectivos para proteger derechos. Respecto al artículo 17 del PIDCP, que protege la privacidad, recomendó que "las personas deberían tener derecho a interponer recursos efectivos cuando sus derechos a la privacidad en línea sean presuntamente vulnerados" (CDHNU 2014, 61). Este recurso sería presentado ante un órgano independiente que pueda acceder al material y respetar las garantías del debido proceso. De la misma forma, presume la existencia de un órgano externo con capacidad de supervisión y medios vinculantes para controlar los excesos.

En el 2010, la misma Relatoría emitió informe sobre las buenas prácticas de garantía y respeto de los derechos humanos desde los servicios de inteligencia. La recomendación práctica N.º 24 sugirió que los organismos de inteligencia evalúen constantemente la exactitud y pertinencia de la información que recaban (CDHNU 2010). A pesar de la obligación de los sistemas de inteligencia de suprimir datos impertinentes para su mandato "es importante que esto no vaya en detrimento de la labor de los organismos de supervisión o de las posibles actuaciones judiciales" (CDHNU 2010, 38). La información no relevante o recolectada por error debería ser destruida sin menoscabar la capacidad para reclamar una violación del derecho a la privacidad.

Como ya se indicó, la normativa ecuatoriana no desarrolla el proceso de notificación a las personas cuyos derechos fueron vulnerados durante operaciones de inteligencia. La regulación sobre la recolección de información de terceras personas no vinculadas a las investigaciones es inadecuada. La información recolectada puede ser eliminada sin que las personas involucradas hayan tenido acceso a las evidencias. Estas circunstancias implican que no existe un recurso efectivo para reparar las violaciones del derecho a la privacidad en internet, tal como mencionamos en el anterior acápite.

A mediados del 2014, la OACDH emitió un informe sobre el derecho a la privacidad en la era digital. La OACDH recordó la observación general N.º 16 del Comité de Derechos Humanos sobre el derecho a la intimidad del PIDCP y resaltó que su limitación puede ocurrir solo si es legal y no arbitraria (CDH 1988). Con relación a la legalidad y arbitrariedad, una restricción a la privacidad podría ser ilegal si contraría los principios de proporcionalidad y razonabilidad para alcanzar un objetivo legítimo en una sociedad democrática, en la misma línea que el sistema interamericano (CDHNU 2014).

En este mismo informe, la OACNUDH estableció que cualquier limitación al derecho a la privacidad "debe estar prevista en la ley, y la ley debe ser lo suficientemente accesible, clara y precisa para que una persona pueda leerla y saber quién está autorizado a realizar actividades de vigilancia de datos y en qué circunstancias" CDHNU 2014). La LSPE no establece de forma clara y precisa quién realiza las actividades de vigilancia. Los organismos de inteligencia pueden solicitar una intercepción de comunicaciones, pero no se determina cuáles entidades estatales tienen estas competencias (LSPE, art. 20).

Algunas agrupaciones no contempladas explícitamente en la ley, como aquellas que conforman los subsistemas de inteligencia militar, la Unidad de Inteligencia Financiera o el Departamento de Inteligencia Tributaria del Servicio de Rentas Internas, podrían solicitar la intercepción de comunicaciones durante operaciones de inteligencia. Las entidades del sistema nacional de inteligencia están dictaminadas en el reglamento, y este hecho rompe la reserva de ley. Además, no existe claridad respecto a las unidades de los subsistemas de inteligencia que ejecutan las operaciones. Por ej., desde el año 2019, el estatuto orgánico que describe las unidades y competencias del CIES tiene el carácter de reservado (CIES, art. 1) Sin una definición clara de los actores que pueden interceptar comunicaciones y ante la reserva de los procedimientos internos de cada institución en operaciones de vigilancia, las circunstancias para autorizar operaciones de inteligencia son opacas.

El informe de la OACNUDH del 2014 recomendó la aplicación de medidas de supervisión externa y civil, desde todos los poderes del Estado, para evitar prácticas arbitrarias o ilegales que vulneren la privacidad (CDHNU 2014). Un control independiente es necesario "a fin de garantizar la existencia de una rigurosa supervisión del uso de técnicas intrusivas de vigilancia y del procesamiento de la información personal" (CDHNU 2009, 62).

Estas recomendaciones sugieren la intervención de una institución civil independiente de los organismos de inteligencia y del poder ejecutivo con "la autoridad legal para consultar todos los archivos y documentos pertinentes, inspeccionar los locales de los servicios de inteligencia" (CDHNU 2009, 13-14) así como tener acceso al personal que realiza las operaciones de intercepción.

La LSPE carece de un organismo de supervisión independiente, que guarde conformidad con los lineamientos del sistema universal. El artículo 24 establece que la SIN, ahora CIES, debe ser controlado por el poder ejecutivo y rendir cuentas trimestralmente ante la Asamblea Nacional (LSPE). La LSPE y su reglamento no establecen ninguna capacidad para que la Asamblea Nacional pueda acceder a los archivos fruto de la intercepción, a las instalaciones del organismo de inteligencia o contactarse con el personal a cargo de las operaciones. Solo contempla que acuda a la Asamblea Nacional la máxima autoridad del CIES.

Además, la LSPE no garantiza que todos los organismos con capacidad de interceptar comunicaciones rindan cuentas ante la Asamblea Nacional. El

Departamento de Inteligencia Tributaria o la Unidad de Vigilancia del Servicio Nacional de Aduana, que conforman el sistema nacional de inteligencia, podrían solicitar una intervención a las telecomunicaciones (Plan V, 2018). Sin embargo, al no formar parte de los órganos ejecutores de la LSPE (art. 11), estas instituciones no tienen la obligación de rendir cuentas ante la Asamblea Nacional (art. 24). No existe un control horizontal de sus acciones. Tampoco se cumple la reiterada recomendación de la ONU sobre la necesidad de órganos independientes de control externo con capacidad de supervisión eficaz. Esta garantía ayudaría a evitar restricciones arbitrarias e ilegales al derecho a la privacidad.

De esta manera, la LSPE no guarda coherencia con las recomendaciones emitidas por organismos de derechos humanos del sistema universal. Frente al desarrollo de las nuevas tecnologías, fueron establecidos ciertos estándares para resguardar el derecho a la privacidad. Estos determinan elementos esenciales para el respeto al debido proceso, el equilibrio procesal, la publicidad, el manejo adecuado, el procesamiento de la información obtenida en casos de inteligencia y la necesidad de un órgano independiente de supervisión. Sin embargo, la LSPE no establece condiciones mínimas para asegurar que la restricción a la privacidad no menoscabe el derecho a la intimidad del artículo 17 del PIDCP.

CONCLUSIONES Y RECOMENDACIONES

En el Ecuador, la regulación de la intercepción de comunicaciones durante operaciones de inteligencia no establece las garantías necesarias para prevenir violaciones al derecho a la privacidad. El procedimiento de la LSPE, que faculta a los organismos de inteligencia a restringir la privacidad personal, no respeta la obligación de orientar la estructura estatal para garantizar los derechos humanos. La privacidad, como una expresión de la dignidad humana y una de las garantías para la convivencia en una sociedad democrática, está sujeta a limitaciones potencialmente arbitrarias e ilegales del Estado sobre el control de la circulación de la información.

Los elementos esenciales del derecho a la privacidad no son protegidos por la LSPE en la restricción de la vida personal y familiar. La intercepción de las telecomunicaciones no respeta los principios y derechos de la Constitución del 2008. En la LSPE, la regulación de la intercepción de las comunicaciones es laxa, no garantiza la transparencia del juicio y las garantías procesales mínimas. En el caso de una intervención arbitraria, no existen las garantías del debido proceso para reconocer y reparar una vulneración de derechos y lograr una efectiva protección del derecho a la privacidad. El Estado tiene una capacidad de acceso y control a la información personal excesiva. En ciertos casos, las justificaciones para la restricción de la privacidad resultan ambiguas e indeterminadas en el contexto de la protección de la seguridad integral.

La visión de seguridad integral, que en la actualidad busca proteger la seguridad nacional, es incompatible con los estándares de los derechos humanos y supone un riesgo de politización y abusos. En efecto, las políticas públicas de seguridad vigentes, acompañadas de la regulación en la LSPE, rompen con la jerarquía de intereses democráticos aceptables, al ubicar a los derechos humanos como un punto de referencia y no como un concepto transversal. Esta situación legal permite la aquiescencia de acciones que podrían menoscabar el contenido del derecho a la privacidad, con el objetivo de garantizar la seguridad nacional y la estabilidad del Gobierno en el poder. Los organismos de inteligencia pueden emprender acciones para restringir, de manera ilegal o arbitraria, la intimidad de las personas, en gran parte debido a la discrecionalidad con la que se maneja el concepto de seguridad nacional, con un riesgo de politización.

En este contexto, varios organismos internacionales de derechos humanos han establecido estándares sobre la protección de la privacidad en el ámbito de las nuevas tecnologías de la información y la comunicación, frente a restricciones ilegales y arbitrarias del Estado. Estas recomendaciones no han sido

incorporadas en la LSPE. En efecto, en el sistema interamericano de derechos humanos y en la ONU, varias decisiones y pronunciamientos establecen condiciones puntuales sobre la excepcionalidad de la limitación del derecho a la privacidad, en caso de operaciones de inteligencia.

La intercepción de comunicaciones tal como consta en la LSPE irrespeta los estándares internacionales vinculantes sobre la obligación de respeto del derecho a la privacidad en una sociedad democrática. La concepción de seguridad integral de la Constitución del Ecuador, cuya centralidad radica en la protección de los derechos humanos, es incompatible con aquella restricción de la privacidad que va unida a la inaceptable justificación que pretexta la necesidad de obtener información de inteligencia.

El irrespeto de los estándares del sistema universal e interamericano sobre la protección del derecho a la privacidad se manifiesta principalmente en la falta de mecanismos de protección y garantías del debido proceso; la carencia de recursos para determinar y acceder a la justicia en caso de una vulneración del derecho a la privacidad, inclusive para terceros afectados; las restricciones inadecuadas al principio de publicidad; la falta de mecanismos de control, de rendición de cuentas y de transparencia eficaces y vinculantes; así como la opacidad sobre los actores intervinientes y los procedimientos establecidos en la LSPE.

En el año 2014, el país apoyó una resolución de la Asamblea General de Naciones Unidas que llamó a los Estados a revisar su legislación con relación a la intercepción y recolección de datos, a través de comunicaciones digitales, con miras a proteger el derecho a la privacidad. Esta resolución alentó el establecimiento de órganos independientes de control, que aseguren la transparencia y rendición de cuentas (AGNU 2014). En el 2020, el Ecuador reafirmó la vigencia internacional de los derechos humanos en el ámbito de las operaciones en ciberespacio, incluidas las acciones de inteligencia (Hollis 2020). Aún está pendiente un debate informado sobre la actualización de los marcos normativos sobre la intercepción de comunicaciones para fines de inteligencia, de esta que se guarde conformidad con los estándares que el Ecuador ha impulsado en foros multilaterales.

Los sistemas interamericano y universal han desarrollado extensas recomendaciones sobre vigilancia y privacidad que permiten al Estado revitalizar su sistema nacional de inteligencia para generar mayor confianza y legitimidad en el sector de seguridad. En este sentido, la aceptación de la propuesta de visita al Ecuador por parte del relator especial sobre la intimidad (Cannataci 2019) permitiría recibir recomendaciones específicas sobre la mejora de los mecanismos de protección del derecho a la privacidad en el contexto de operaciones de inteligencia y el desarrollo de nuevas tecnologías de información y comunicación.

BIBLIOGRAFÍA

Ávila, Ramiro. 2012. «Evolución de los derechos fundamentales en el constitucionalismo ecuatoriano». Ponencia pronunciada en el Congreso Ecuatoriano de Historia. http://repositorio.uasb.edu.ec/bitstream/10644/3015/1/%C3%81vila%2C%20R-CON-008-Evoluci%C3%B3n.pdf

_____. 2009. «Del Estado legal de derecho al Estado constitucional de derechos y justicia». *Anuario de Derecho Constitucional Latinoamericano 2009*, editado por Gisela Elsner: 775-793. Montevideo: Fundación Konrad Adenauer.

_____. 2009. «Los principios de Aplicación de los Derechos». *Nuevas instituciones del Derecho Constitucional ecuatoriano*, editado por Luis Saavedra, 27-58. Quito: INREDH.

AGNU. Ver Asamblea General de las Naciones Unidas. 2014. *El derecho a la privacidad en la era digital*. N.º A/RES/69/166. Nueva York: Organización de las Naciones Unidas.

Benavides, Gina y Gardenia Chávez. 2013. *Horizonte de los derechos humanos en el 2012*. Quito: Universidad Andina Simón Bolívar.

Bigo, Didier, Sergio Carrera y Elspeth Guild. 2015. «The EU and its Counter-Terrorism Policies after the Paris Attacks». N.° 84, noviembre 2015. http://aei.pitt.edu/69691/1/No_84_EU_Responses_to_Paris_0.pdf

Cannataci, Joseph. 2019. «Experto de la ONU en privacidad seriamente preocupado por el comportamiento de Ecuador en los casos Assange y Moreno». https://www.ohchr.org/SP/NewsEvents/Pages/DisplayNews.aspx?NewsID=24646&LangID=S

CDH. Ver Comité de Derechos Humanos. 1988. "Observación General N.º 16, Artículo 17– Derecho a la intimidad", N.º HRI/GEN/1/Rev.7. Ginebra: Organización de las Naciones Unidas.

CDHNU. Ver Consejo de Derechos Humanos. 2018. "Report of the Special Rapporteur on the right to privacy", N.° A/HRC/37/62. Ginebra: Organización de las Naciones Unidas.

_____. 2014. "The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights", Nro. A/HRC/27/37. Ginebra: Organización de las Naciones Unidas.

_____. 2014. "Informe del Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo: Promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo". N.º A/69/397. Ginebra: Organización de las Naciones Unidas.

_____. 2010. "Informe del Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo: Recopilación de buenas prácticas relacionadas con los marcos y las medidas de carácter jurídico e institucional que permitan garantizar el respeto de los derechos humanos por los servicios de inteligencia en la lucha contra el terrorismo, particularmente en lo que respecta a su supervisión". N.º A/HRC/14/46. Ginebra: Organización de las Naciones Unidas.

_____. 2009. "Informe del Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo". Nro. A/HRC/13/37. Ginebra: Organización de las Naciones Unidas.

CIDH. Ver Comisión Interamericana de Derechos Humanos. 2009. *Informe sobre seguridad ciudadana y derechos humanos*, N.º OEA/Ser.L/V/II. Doc. 57. Washington D.C.: Comisión Interamericana de Derechos Humanos.

CIES. Ver Centro de Inteligencia Estratégica. 2019. *Plan Específico de Inteligencia 2019-2030*. Quito: Centro de Inteligencia Estratégica. https://www.defensa.gob.ec/wp-content/uploads/downloads/2019/07/plan-nacional-inteligencia-web.pdf

Corral, Hernán. 2000. «Configuración jurídica del Derecho a la privacidad». Revista Chilena de Derecho, Vol. 27 N.°2: 331-355.

CorteIDH. Ver Corte Interamericana de Derechos Humanos. 1986. Opinión Consultiva OC-6/86. San José: Corte Interamericana de Derechos Humanos.

CTITF. Ver Working Group on Protecting Human Rights while Countering Terrorism. 2014. *Basic Human Rights Reference Guide: Right to a Fair Trial and Due Process in the Context of Countering Terrorism*. Nueva York: Organización de las Naciones Unidas.

DPE. Ver Defensoría del Pueblo del Ecuador. 2015. *Criterios y estándares del derecho a la igualdad y no discriminación para la incidencia normativa y la incorporación del enfoque de derechos humanos en las políticas públicas*. Quito: Defensoría del Pueblo.

Escalante, Fernando. 2004. *El derecho a la privacidad*. México D.F.: Instituto Federal de Acceso a la Información Pública.

Froomkin, Michael. 2000. «The death of Privacy?». Stanford Law Review. Vol. 52: 1461-1543.

Greenwald, Glenn. 2014. *Snowden: Sin un lugar donde esconderse*. Bogotá: Editora Géminis.

Hollis, Duncan. 2020. "Derecho Internacional y operaciones cibernéticas del Estado: mejora de la transparencia". Rio de Janeiro: Organización de los Estados Americanos. https://www.oas.org/en/sla/iajc/docs/CJI_doc_603-20_rev1.pdf

Hurtado, Francisco. 2010. «La ley de seguridad y sus implicaciones para derechos humanos». *¿Estado constitucional de derechos? Informe sobre derechos humanos Ecuador 2009*: 101-118. Quito: Universidad Andina Simón Bolívar y Abya-Yala.

MDG. Ver Ministerio de Gobierno. 2019. *Plan Nacional de Seguridad Ciudadana y Convivencia Pacífica 2019-2030*. Ecuador: Ministerio de Gobierno.

Melish, Tara. 2003. *La Protección de los Derechos Económicos, Sociales y Culturales en el Sistema Interamericano de Derechos Humanos*. Quito: CDES.

Ministerio de Defensa Nacional. 2019. *Plan Nacional de Seguridad Integral 2019-2030*. Quito: Ministerio de Defensa Nacional. https://www.defensa.gob.ec/wp-content/uploads/downloads/2019/07/plan-matriz-web.pdf 108

Nieves, María. 2017. «La protección de la información en la sociedad tecnológica». Revista Araucaria Universidad de Huelva, N.°18: 85-115.

Nissenbaum, Helen. 2010. *Privacidad amenazada: tecnología, política y la integridad de la vida social*. México: Océano.

Ordóñez, María y Galo Cruz. 2017. «La inteligencia militar ecuatoriana en la sociedad del riesgo». URVIO, N.º 21: 56-69. https://revistas.flacsoandes.edu.ec/urvio/article/view/2964/2015

Plan V. 2018. «¿Ecuador tiene una estructura de inteligencia debilitada?». Plan V, 28 de febrero. https://www.planv.com.ec/historias/politica/ecuador-tiene-una-estructura-inteligencia-debilitada

Post, Robert. 2001. «Three Concepts of Privacy». Yale Law School Faculty Scholarship Series, N.° 185. https://digitalcommons.law.yale.edu/fss_papers/185

Ricaurte, Paola. 2015. «Desafíos de la acción colectiva en la era post-Snowden: lecturas desde América Latina». *Teknocultura*, Vol. 12 N.º 3: 429-447. http://revistas.ucm.es/index.php/TEKN/article/view/51340/47835

Rivera, Freddy y Katalina Barreiro. 2011. *Inteligencia estratégica y prospectiva*. Quito: FLACSO.

Rivera, Freddy. 2019. «¿Qué tan nueva es la actual Política de la Defensa?». Plan V, 16 de enero. https://www.planv.com.ec/historias/sociedad/que-tan-nueva-la-actual-politica-la-defensa

_____. 2017. «Inteligencia estratégica e inteligencia política: los claro-oscuros del caso ecuatoriano». *Inteligencia estratégica contemporánea*, editado por David Andrade Aguirre: 133-148. Sangolquí: Universidad de las Fuerzas Armadas ESPE.

_____. 2012. *La seguridad perversa: Política, democracia y derechos humanos en Ecuador*. Quito: FLACSO.

Rodríguez, Víctor. 1998. «El debido proceso legal y la Convención americana sobre derechos humanos». En *Liber Amicorum*, coordinado por Héctor Fix-Zamudio, 1295-1328. San José: Corte Interamericana de Derechos Humanos.

SENPLADES. Ver Secretaría Nacional de Planificación y Desarrollo. 2017. *Plan Nacional de Desarrollo 2017-2021*. Quito: Secretaría Nacional de Planificación y Desarrollo.

Snowden, Edward. 2019. *Permanent Record*. Londres: Macmillan.

Trujillo, Julio. «Funciones normativas de la Constitución». *Constitucionalismo contemporáneo, teoría, procesos, procedimientos y retos*. Quito: Universidad Andina Simón Bolívar.

Whitman, James. 2004. «The Two Western Cultures of Privacy: Dignity Versus Liberty». The Yale Law Journal, N.º 113.6: 1151-1221.

Normativa y jurisprudencia

CADH. Ver Convención Americana sobre Derechos Humanos. 1969. Organización de Estados Americanos: Conferencia Especializada Interamericana sobre Derechos Humanos.

CC. Ver Corte Constitucional del Ecuador. Sentencia N.°001-10-SIN-CC. Casos N.º 0008-09-IN y 0011-09-IN. Ecuador: Corte Constitucional del Ecuador.

CE. Ver Constitución de la República del Ecuador. 2008. Ecuador: Asamblea Nacional Constituyente. Registro Oficial 449, 20-X-2008.

CIES. Ver Centro de Inteligencia Estratégica. 2019. Ecuador: Centro de Inteligencia Estratégica. Resolución N.º CIES-R-001-2019 del 2-I-2019.

COESCOP. Ver Código Orgánico de las Entidades de Seguridad Ciudadana y del Estado. Ecuador: Asamblea Nacional. Registro Oficial Suplemento 19 de 21-VI-2017.

COIP. Ver Código Integral Penal. 2014. Ecuador: Asamblea Nacional. Registro Oficial Suplemento 180 de 10-II-2014.

Corte IDH. Ver Corte Interamericana de Derechos Humanos. Caso Tristán Donoso vs Panamá. Sentencia de fondo del 27-I-2009.

_____. Ver Corte Interamericana de Derechos Humanos. Caso Velásquez Rodríguez vs Honduras. Sentencia de Fondo, del 29 de julio de 1988.

DE 536. Ver Decreto Ejecutivo 536. 2018. Ecuador: Presidencia de la República. Registro Oficial Suplemento 358 de 30-X-2018.

DUDH. Ver Declaración Universal de Derechos Humanos. 1948. NY: Asamblea General de la ONU. Resolución N.º 217 A (III).

LSPE. Ver Ley de Seguridad Pública y del Estado. 2009. Ecuador: Asamblea Nacional. Registro Oficial Suplemento 35 de 28-IX-2009.

PIDCP. Ver Pacto Internacional de Derechos Civiles y Políticos. 1966. NY: Asamblea General de la ONU. Resolución N.°2200-A-XXI.

Ministerio de Defensa Nacional. Política de la Defensa Nacional del Ecuador. Decreto Ejecutivo 633. 2019. Ecuador: Presidencia de la República. Registro Oficial 412 de 23-I-2019.

Reglamento LSPE. Ver Reglamento a la Ley de Seguridad Pública y del Estado. 2010. Ecuador: Presidencia de la República. Decreto Ejecutivo 48. Registro Oficial Suplemento 290 de 30-IX-2010.