La necesidad de incorporar al agente encubierto cibernético en la Legislación Ecuatoriana[1]

The importance of incorporating the undercover agent in the Ecuadorian Legislation

Gladis Proaño Reyes[2]
Universidad San Francisco de Quito

Resumen

Pactar con la práctica de actos criminales para descubrir un delito será motivo de análisis, por lo que los principios básicos de legalidad, especialidad, subsidiariedad, proporcionalidad, control jurisdiccional y seguridad jurídica deberán probarse cuando sea necesario la infiltración de un agente encubierto en organizaciones delictivas que utilizan el ciberespacio. La tecnología está desplazando al agente encubierto en persona; los medios tecnológicos permiten de manera invisible allanar y estar presente en el lugar de los hechos, escanear, describir, escuchar y recoger información entre otras actividades rebasando los límites geográficos y las fronteras, ante delitos globalizados que requiere de la cooperación internacional y la asistencia mutua entre países para combatir en el ciberespacio en los que debe intervenir el agente encubierto cibernético.

Palabras clave

Agente encubierto / Agente encubierto cibernético / Medios tecnológicos / Delincuencia organizada / Delitos cibernéticos.

Summary

Settling criminal acts to uncover another crime shall be reason for investigation. In these circumstances, the basic principles of law, specialty, subsidies, proportion, jurisdictional control and legal security will need to be justified before infiltrating an undercover agent in an organized crime entity that uses cyberspace. Technology is replacing the participation of undercover agents, as technical devices allow an invisible way to observe and be present, scan, describe, listen and collect information from a potential crime scene, regardless of geographical limits and borders. This is particularly important when global crimes require international cooperation and mutual assistance between countries to deal with cyberspace that need the intervention of a cyber undercover agent.

Keywords

Undercover agent / Cyber undercover agent / Technical devices / Organized crime / Cybercrime.

1 Recibido: 06/06/2018 – Aceptado: 26/09/2018

2 Doctora en Jurisprudencia, Magíster en Derecho Penal y Criminología y Ph.D en Educación. Profesora de la Universidad San Francisco de Quito y posgrado de la Universidad Andina Simón Bolívar. Capacitadora Internacional en temas de Delincuencia Organizada Transnacional. Correo electrónico: proanoreyes@yahoo.com

Gladis Proaño Reyes (2018). La necesidad de incorporar al agente encubierto cibernético en la Legislación Ecuatoriana, *Iuris Dictio 22,* 217-228.
ISSN 1390-6402 / e-ISSN 2528-7834.
DOI: http://dx.doi.org/10.18272/iu.v22i22.1127

1. Introducción

La tecnología ha estado ligada al desarrollo de la humanidad, debemos anotar, siguiendo a Castells (2006), que la sociedad actual de espacios virtuales y cibernéticos, que él denomina "sociedad red", se diferencia de los anteriores desarrollos históricos de las tecnologías de la información y la comunicación (como la imprenta, el telégrafo o el teléfono no digital) por tres características fundamentales de las tecnologías que forman el núcleo del sistema: a) su capacidad autoexpansiva de procesamiento y de comunicación en términos de volumen, complejidad y velocidad; b) su capacidad de recombinar basada en la digitalización y en la comunicación recurrente; y c) su flexibilidad de distribución mediante redes interactivas y digitalizadas.

En esta sociedad red, las posibilidades de que sean cometidos delitos de variada naturaleza son prácticamente infinitas, sin fronteras y sin concepciones de jurisdicción y competencia delimitadas por la Constitución y la legislación procesal de cada país. Las medidas y operaciones que son requeridas para contener estos delitos en el ciberespacio deben trascender la regulación tradicional.

La figura del agente encubierto lejos de estar siendo desplazada por la tecnología, se asiste de ella para lograr los fines de su acción, sin poner en riesgo su integridad personal, pudiendo llegar al lugar, escuchar, mirar, identificar a los sospechosos, examinar, conseguir y llevarse indicios que le sirvan como elementos de convicción en un proceso penal de formas antes no conocidas.

Claro está, siempre persistirán los problemas y las dudas sobre la legalidad en la obtención de estas informaciones, sobre todo por tratarse de un medio extraordinario y excepcional, en el que haciendo uso de artimañas tales como la suplantación de identidad y la interceptación de las comunicaciones se busca colocar ante la justicia personas sospechosas de la comisión de algún ciberdelito.

2. Consideraciones Generales

2.1. Las Técnicas Especiales de Investigación

Las Técnicas Especiales de Investigación se encuentran determinadas en la sección tercera del libro segundo del Código Orgánico Integral Penal (COIP), vigente en el Ecuador desde el 10 de agosto de 2014. Así se ubican disposiciones que posibilitan: la interceptación de las comunicaciones o datos informáticos (artículos 476 y ss), y las operaciones investigativas con agentes encubiertos e informantes (artículos 483 y ss). Si bien las Técnicas Especiales de Investigación no se encuentran definidas en el COIP, la fórmula empleada en la norma asemeja la contenida en la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional.

Como su nombre indica, las Técnicas de Investigación Especiales, son "especiales" en la medida de que su utilización puede causar lesiones o agravios a derechos fundamentales de los ciudadanos, de allí que, su empleo debe ser considerado igualmente de manera "especial" o, a tenor de la norma penal "de manera excepcional[3]" y cuando se encuentre ampliamente justificada su autorización.

---

3 COIP, artículo 483.- "Operaciones encubiertas.- En el curso de las investigaciones de manera excepcional, bajo la dirección de la unidad especializada de la Fiscalía, se podrá planificar y ejecutar con el personal del Sistema especializado integral de investigación, de medicina legal y ciencias forenses, una operación encubierta y autorizar a sus agentes para involucrarse o introducirse en organizaciones o agrupaciones delictuales ocultando su identidad oficial, con el objetivo de identificar a los participantes, reunir y recoger información, elementos de convicción y evidencia útil para los fines de la investigación.

El agente encubierto estará exento de responsabilidad penal o civil por aquellos delitos en que deba incurrir o que no haya podido impedir, siempre que sean consecuencia necesaria del desarrollo de la investigación y guarden la debida proporcionalidad con la finalidad de la misma, caso contrario será sancionado de conformidad con las normas jurídicas pertinentes" (Énfasis mío).

En el catálogo descrito de las Técnicas de Investigación Especiales, los agentes encubiertos tienen un lugar de honor en cuanto a su estudio, ya que la cantidad de derechos que se encuentran vulnerados en estas operaciones, solo es justificable con el número de presuntos delitos que serían detectados y delincuentes aprehendidos.

2.2. Acerca del Agente Encubierto y diferencias con otras figuras

En el Ecuador el agente encubierto es un servidor policial o de la fiscalía de quien se conoce su récord personal y profesional.

El agente infiltrado, nombre dado por Molina Pérez:

> Es un funcionario de la Policía que tiene por misión actuar, dentro de la clandestinidad, en un determinado ambiente criminal para reprimir y prevenir acciones delictivas, y para descubrir a quienes integran la organización criminal, con las tareas y funciones que les vienen atribuidos por la Ley (Molina Pérez, 2009, p. 155).

El agente encubierto, infiltrado o clandestino, se involucra de manera directa con la organización delictual, a descubrir toda la información que sea posible, sobre personas involucradas (activas y pasivas), así como la posible infracción a cometer o que ha sido cometida.

Por su parte, el informante es cualquier persona que provee a la fiscalía o al personal del Sistema Especializado Integral de Investigación, de Medicina Legal y Ciencias Forenses, sobre los antecedentes acerca de la preparación o comisión de una infracción o de quienes han participado en ella. En ambas figuras la identidad de estas personas se encuentra protegida y su revelación constituye delito tipificado y sancionado en el COIP (artículo 273).

La doctrina extranjera se refiere al confidente, entendido como:

> Aquel sujeto que transmite información a quienes están encargados de una investigación penal y que, a cambio de ella, obtiene ciertas ventajas. Puede estar dentro de una organización, o fuera de ella, pero no provoca delitos no está infiltrado con el fin de investigar (Molina Pérez, 2009).

La actividad de los agentes encubiertos, como se recoge en la legislación ecuatoriana, se centra principalmente en la recolección de información y de elementos de convicción haciendo uso de una identidad ficticia, no se plantea que el agente pueda ser provocador de situaciones delictivas, la doctrina consultada (Molina Pérez, 2009) anota que podrá instarlas, convirtiéndose en agente provocador.

3. Los actuales escenarios del crimen y sus implicaciones en la actividad de los Agentes Encubiertos

3.1. El Cibercrimen y su atención en Ecuador

El Convenio sobre la Ciberdelincuencia, también conocido como Convenio de Budapest del año 2001[4], si bien inicialmente fue aprobado por el Consejo de Europa, en la actualidad

4 Dentro de los antecedentes de este Convenio, el autor Juan Pablo Albán Alencastro cita "los esfuerzos realizados por la Organización para la Cooperación y el Desarrollo Económicos en Europa (OCDE) desde 1983, cuando emprendió un estudio sobre la posibilidad de aplicar y armonizar en el plano internacional las leyes penales, a fin de luchar contra el problema del uso indebido de los programas de computación; todo este esfuerzo concluyó con la publicación, en 1986, del informe

cuenta con la suscripción y ratificación de más de 56 países incluyendo no europeos, en la búsqueda de cooperación para la lucha contra delitos informáticos, que son cometidos en un ambiente intangible; no en un mundo de átomos y de células, sino digital, conocido como ciberespacio (Goodman, 2003, p. 8).

Siguiendo al profesor Albán Alencastro, entre los aspectos más notables del Convenio de Budapest se encuentran:

(a) la promoción de la armonización del derecho penal sustantivo de los Estados miembros en materia de delitos cibernéticos, así como la identificación de ciertas infracciones particularmente graves que deberían merecer atención prioritaria: lo cual se evidencia con la incorporación de un capítulo dedicado a la terminología; y otro capítulo relativo a la tipificación de los delitos: delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos; delitos informáticos propiamente dicho; delitos relacionados con el contenido: donde se ubica la pornografía infantil; delitos con infracciones de la propiedad intelectual y de los derechos afines; y otras formas de responsabilidad y de sanción (tentativa y complicidad y la responsabilidad de las personas jurídicas);
(b) la propuesta de parámetros procesales mínimos para la investigación y sanción de tales conductas, así se consagran disposiciones sobre: ámbitos de aplicación de las disposiciones de procedimientos; condiciones y salvaguardas; conservación rápida, registro, confiscación y obtención en tiempo real de datos informáticos almacenados; orden de presentación;
(c) la creación de mecanismos de cooperación a nivel europeo para el combate a la ciberdelincuencia. Se enlistan los siguientes principios: generales de la cooperación internacional, relativos a la extradición, referentes a la asistencia mutua; información espontanea; así como el establecimiento de procedimientos concernientes a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables; confidencialidad y restricciones de uso.

Si bien el Ecuador no es parte de este convenio, no significa que esta materia no haya sido tratada, y cada vez con mayor importancia y nivel investigativo. Así, en octubre del año 2008, se desarrolló el evento "Cibercriminalidad en Ecuador"[5], el cual tuvo por objeto analizar los delitos más frecuentes en América Latina cometidos por vías informáticas, así como las principales violaciones a la propiedad intelectual, delitos en comercio electrónico, firmas y mensajes de datos, pornografía infantil, entre otros.

Ahora bien, el COIP no regula con especial tratamiento esta materia, a decir de la doctrina consultada:

titulado "Delitos de Informática" que examina el marco jurídico entonces vigente en diversos países europeos, marco que potencialmente podía ser utilizado para enfrentar esta forma de criminalidad, así como una serie de propuestas mínimas de reforma y ampliación a partir de ejemplos de uso indebido de sistemas informáticos que los países podrían prohibir mediante el derecho penal, por ejemplo, el fraude y la falsificación informática, la alteración de datos, el acceso no autorizado, la interceptación y la reproducción no autorizada de programas y aplicaciones. También el Consejo de Europa desde 1963 a través de su Legal Advisory Board y desde 1997 con el Plan de Acción adoptado por los Jefes de Estado y de Gobierno del Consejo de Europa con ocasión de su Segunda Cumbre (Estrasburgo, 10 y 11 de octubre de 1997), empezó a desarrollar una estrategia para buscar respuestas comunes ante la proliferación de las nuevas tecnologías de la información. Tales esfuerzos llegaron a un consenso, en abril de 2000, y se publicó el "Proyecto de Convención sobre el Delito Cibernético" (Albán Alencastro, 2016, pp. 26-27).

5 Para información sobre el mismo, consultar:
<http://www.coberturadigital.com/2008/10/28/cibercriminalidad-en-ecuador-encuentro-de-delitos-informaticos/>.

> En todo caso, lo que el legislador ecuatoriano ha hecho frente al fenómeno de la cibercriminalidad es identificar ciertas conductas que podrían cometerse empleando medios informáticos y solo excepcionalmente se ha ocupado de tutelar directamente la integridad, disponibilidad y/o accesibilidad de los sistemas informáticos y los datos alojados en ellos. También resulta notable que solo en un tipo penal se hace una alusión directa al Internet[6] (Albán Alencastro, 2016, p. 33).

Estos temas del diario acontecer del país y del mundo deben ser trabajados con rigor y es menester su constante revisión dada la "inseguridad informática, utilizada como estrategia táctica y estratégica por el crimen organizado", lo cual se presenta como un problema que puede alcanzar inmensurables aspectos o ámbitos, pero que claro está, afecta a todos los que utilizamos (no importa para qué) los medios informáticos para comunicarnos y muy especialmente los que tienen acceso a Internet[7].

INTERPOL[8] en la lucha contra los ciberdelincuentes apoya con soporte operacional e investigativo, inteligencia cibernética y análisis, forense digital, innovación e investigación. Ecuador, como miembro activo desde más de cincuenta años, debe recurrir a las oportunidades tecnológicas que ofrece ese Organismo internacional para enfrentar las ciberamenazas que afectan principalmente niños, niñas y adolescentes quienes ante la ausencia de afecto terrenal acuden al ciberespacio y en redes oscuras encuentran respuestas que en muchos casos les encaminan e instigan a la muerte.

EUROPOL[9] junto al EC3[10] se han aliado a Interpol para enfrentar los desafíos de perseguir a las actividades ilegales en línea; la IOCTA[11] en su informe 2017 destaca algunos éxitos operativos en la lucha contra los ciberdelitos, como la eliminación de los mayores mercados Darknet, AlphaBay, Hansa y el desmantelamiento de la red Avalancha en la que participaron 40 países, recomendando que ante la creciente amenaza de la ciberdelincuencia se requiere una legislación específica que permita la presencia de la ley y la acción en un entorno en línea. La falta de una legislación adaptada está causando pérdida de pistas de investigación y la capacidad de procesar eficazmente la actividad criminal en línea, concluye; precisamente esa advertencia debe apuntar a contar con una legislación universal.

De allí que, más recientemente, el 24 de octubre del 2017 en Quito, los integrantes del Programa de Lucha Contra el Crimen Organizado Transnacional —PACcTO—[12], se

6 COIP, artículo 230.- "Interceptación ilegal de datos.- Será sancionada con pena privativa de libertad de tres a cinco años: […] 2. La persona que diseñe, desarrollo, 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 […]."

7 "Si bien Internet y la web han abierto la puerta a nuevas experiencias de redes sociales, amigos y contactos profesionales, también es una 'inmensa' base de datos nuestros que utilizando las herramientas adecuadas y alguna seña particular, es capaz de establecer datos privados o tan personales que se piensa están resguardados en sitios donde tenemos registradas fotos, documentos, entre otros elementos" (Cano, 2007, p. 176).

8 La Organización Internacional de Policía Criminal es la mayor organización de policía internacional, con 192 países miembros, por lo cual es una de las organizaciones internacionales más grandes del mundo, tan sólo por detrás de las Naciones Unidas.

9 La Oficina Europea de Policía es el órgano encargado de facilitar las operaciones de lucha contra la delincuencia en el seno de la Unión Europea.

10 Centro Europeo de Cibercrimen creado el 11 de enero de 2011.

11 Evaluación de la Amenaza del Crimen Organizado, en sus siglas en inglés IOCTA.

12 Programa financiado por la Unión Europea, que reúne a países como: Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Cuba, Ecuador, El Salvador, Guatemala, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, Uruguay, Venezuela, con la participación activa de la Comunidad de Policías de América —AMERIPOL—, Red Iberoamericana de Cooperación Jurídica Internacional —IberRed—, Grupo de Acción Financiera de Latinoamérica —GAFILAT—, Organización

reunieron precisamente para tratar sobre el delito de pornografía infantil e identificar las falencias normativas presentes en los delitos sexuales contra niños, niñas y adolescentes, como es la prescripción del delito de abuso sexual a menores de edad, (que en el caso particular del Ecuador se decidió a través de un referéndum el 4 de febrero de 2018 en el que se determinó su imprescriptibilidad).

La obtención de indicios y elementos de convicción para combatir los delitos sexuales es una urgente preocupación expresada por los delegados de los países, debido a que rebasa a cualquier actuación policial y del agente encubierto físico-humano para perseguir a pedófilos y pederastas que ya no delinquen en terreno real, sino que se ha convertido en un internauta utilizando Internet y por ende se han trasladado a un ciberespacio.

La preocupación surge porque la fijación del lugar en el que se comete el acto delictivo no coincide con el que se produce el resultado, siendo éste múltiple, debido a que de manera inidentificable los consumidores internautas se multiplican en diferentes países y territorios en los que puede materializarse; es ahí, donde la jurisdicción y la competencia se convierten en motivo de análisis, ya que cada ámbito de acción delictual, desconoce los límites territoriales planteados y organizados en la Constitución[13], en el COIP[14] e incluso en el Reglamento para la Implementación y Funcionamiento del Sistema de Vigilancia Técnica Electrónica[15].

Velasco San Martín (2012) realiza un profundo estudio pragmático de la problemática de la jurisdicción y competencia frente a los delitos cometidos a través de sistemas de cómputo e Internet, refiriéndose a Latinoamérica, orienta a que todos los países utilicen un mismo leguaje legislativo para armonizar sus procedimientos con miras a combatir los delitos aéreos.

Dado el auge de la ciberdelincuencia y otros delitos relacionados con evidencia electrónica, la incertidumbre sobre la jurisdicción, hace necesaria y de manera excepcional,

---

Internacional de Policía Criminal —INTERPOL—, el Mercado Común del Sur —MERCOSUR—, el Sistema de la Integración Centroamericana —SICA— y la Asociación Iberoamericana de Ministerios Públicos —AIAMP—.

13 Artículo 4.- "El territorio del Ecuador constituye una unidad geográfica e histórica de dimensiones naturales, sociales y culturales, legado de nuestros antepasados y pueblos ancestrales. Este territorio comprende el espacio continental y marítimo, las islas adyacentes, el mar territorial, el Archipiélago de Galápagos, el suelo, la plataforma submarina, el subsuelo y el espacio suprayacente continental, insular y marítimo. Sus límites son los determinados por los tratados vigentes. El territorio del Ecuador es inalienable, irreductible e inviolable. Nadie atentará contra la unidad territorial ni fomentará la secesión. La capital del Ecuador es Quito. El Estado ecuatoriano ejercerá derechos sobre los segmentos correspondientes de la órbita sincrónica geoestacionaria, los espacios marítimos y la Antártida".

Artículo 242.- "El Estado se organiza territorialmente en regiones, provincias, cantones y parroquias rurales. Por razones de conservación ambiental, étnico-culturales o de población podrán constituirse regímenes especiales. Los distritos metropolitanos autónomos, la provincia de Galápagos y las circunscripciones territoriales indígenas y pluriculturales serán regímenes especiales".

14 Artículo 14.- "Ámbito espacial de aplicación. -Las normas de este Código se aplicarán a: 1. Toda infracción cometida dentro del territorio nacional. 2. Las infracciones cometidas fuera del territorio ecuatoriano, en los siguientes casos: a) Cuando la infracción produzca efectos en el Ecuador o en los lugares sometidos a su jurisdicción. b) Cuando la infracción penal es cometida en el extranjero, contra una o varias personas ecuatorianas y no ha sido juzgada en el país donde se la cometió. c) Cuando la infracción penal es cometida por las o los servidores públicos mientras desempeñan sus funciones o gestiones oficiales. d) Cuando la infracción penal afecta bienes jurídicos protegidos por el Derecho Internacional, a través de instrumentos internacionales ratificados por el Ecuador, siempre que no se haya iniciado su juzgamiento en otra jurisdicción. e) Cuando las infracciones constituyen graves violaciones a los derechos humanos, de acuerdo con las reglas procesales establecidas en este Código. 3. Las infracciones cometidas a bordo de naves o aeronaves militares o mercantes de bandera o matrícula ecuatoriana. 4. "Las infracciones cometidas por las o los servidores de las Fuerzas Armadas en el extranjero, sobre la base del principio de reciprocidad".

15 Resolución del Consejo Directivo de la Policía Judicial Nº 001-2012-CDPJ; especial referencia al artículo 2.- "Para la consecución de este reglamento, se crea el Sistema de Vigilancia Técnica Electrónica, SVT-E, que tendrá su sede en la capital de la República del Ecuador y tendrá su ámbito de ejecución a nivel nacional. Estará adscrita a la Dirección Nacional de la Policía Judicial e Investigaciones bajo el control de la Fiscalía y demás organismos de fiscalización" (énfasis mío).

la interacción entre Operarios del sistema de justicia de distintos países para realizar las investigaciones pertinentes para disminuir estos hechos delictivos, siempre en un marco de respeto de derechos humanos (Gilles Bélanger, 2017).

Es por esto que se requiere la intervención del agente encubierto para recabar información ya no como un ser humano que opera en una circunscripción judicial determinada, limitada territorialmente. En el ciberespacio, donde opera la delincuencia globalizada que organiza y ejecuta este tipo de crímenes se precisará ampliar la concepción y la esfera de acción de esta figura[16].

3.2. La Actuación del Agente Encubierto Cibernético

La intervención de un agente encubierto que ya no se encuentra limitado a una circunscripción territorial, sino que pasa a ser un agente encubierto cibernético, digital, *online*, o informático, ejecuta la operación encubierta en un espacio cibernético o virtual, caracterizado por ser ilimitado, exuberante y acéntrico. Sus actuaciones en este entorno de algoritmos y claves alfanuméricas, no colocan su vida en peligro o en riesgo físico por la latente posibilidad de ser identificado, sino que tendrá una identidad virtual, que se nutre el anonimato propicio de Internet.

El agente encubierto en Internet es "encubierto en perfiles falsos", ya que como anota Bueno de Mata (2011), la función de este agente consistiría en la ocultación de la verdadera identidad policial, "con el fin de establecer una relación de confianza que permita al agente integrarse durante un periodo de tiempo prolongado en el mundo en el que los "ciberdelincuentes" actúan con la finalidad primordial, igualmente oculta, de obtener la información necesaria para desenmascarar a los supuestos criminales". Siendo una clara posibilidad para perseguir al ciberdelito y lograr detener aquellos perpetradores de delitos como el *grooming*[17], *ciberbullyng*[18] y el *morphing*[19], entre otros.

16 "La inexistencia de fronteras reales es una de las características intrínsecas de Internet, que ofrece innumerables ventajas y como no podía ser de otro modo, inconvenientes para la persecución de actividades delictivas. En primer lugar, para iniciar cualquier política criminal, hay que conocer cuál va ser el terreno de actuación. […] Pero además, y dado que a la Red se puede acceder desde cualquier parte del mundo prácticamente al instante, el siguiente problema relacionado con la independencia geográfica de Internet lo encontramos en la dificultad de perseguir un ilícito de estas características. Quiérase decir que un sujeto puede cometer un delito contra otro situado a miles de kilómetros del primero, mientas que la información está en otro lugar diferente de éstos. La situación puede llegar a producir una verdadera impunidad, si no se articulan los remedios adecuados" (Díaz Gómez, 2010, pp. 173-174).

17 "El grooming —traducción de la palabra "acicalamiento" en inglés— se define como la captación y manipulación de menores de edad en línea con fines sexuales. Es el proceso por el cual un adulto trata de ganarse la confianza de un niño, niña o adolescente haciéndose pasar por otro menor mediante el uso de servicios y aplicaciones en Internet —salas de chat, redes sociales, juegos en línea y servicios de mensajería instantánea, entre otros—. El proceso no es nuevo, es la técnica que utilizan los pedófilos para minar o socavar moral o psicológicamente al niño con el objetivo de controlarlo emocionalmente" (Sain, 2018).

18 "El ciberacoso es entendido como el daño repetido e intencionado ocasionado a través de medios electrónicos como teléfonos móviles o internet, realizado por un grupo o individuo contra el que la víctima no puede defenderse por sí misma. Debido a los diferentes formatos tecnológicos, los "ciberacosadores" (adultos o menores), muchas veces anónimos (forma indirecta de acoso), realizan amenazas, vejaciones, fotografías intimidantes, hostigamientos, y/o menosprecios hacia sus compañeros/as de pupitre a través de diferentes mecanismos con base tecnológica (p.e., envían fotos, vídeos o mensajes de texto —sms— a través de sus teléfonos móviles, o a través de los ordenadores personales, etc.)" (Félix-Mateo y otros, 2010, pp. 47-48).

19 El morphing es un efecto especial utilizado para modificar el rostro de las personas hasta transforma en el de otras. Este efecto que ha sido utilizado en el cine, por ejemplo, se usa para trucar imágenes de pornografía adulta o incluso, imágenes no pornográficas, en escenas de explotación sexual infantil. La Circular 2/2015, sobre los delitos de pornografía infantil tras la reforma operada por LO 1/2015, la Fiscalía General de España se refiere al morphing, como "la llamada pseudo pornografía infantil (también denominada morphing) no se utiliza realmente al menor o incapaz sino que se abusa de su imagen o voz manipulándola con artificios técnicos. […] En todo caso, para poder considerar penalmente trascendente este tipo de material, será necesario, como en el caso de la pornografía virtual, que sea realista, que trate de aproximarse a la realidad, quedando

Si tan invisible es el delincuente cibernético que comete cualquiera de esos delitos, más invisible debe ser el agente encubierto en este escenario virtual, debe ser universal, para prevenir y combatir el crimen por lo tanto no puede estar identificado. El autor español Federico Bueno de Mata (2011), sobre el agente encubierto en la era digital dice:

> Una figura que si la trasladamos a Internet, debe obligatoriamente cambiar sus características y su *modus operandi* para adaptarlo a los entornos virtuales, pero sin hacer que pierda su esencia. Una esencia polémica y muy debatida basada en el engaño y con la que se trataría de utilizar técnicas usadas para delinquir como técnicas a su vez de investigación o combate de este tipo de delincuencia (Bueno de Mata, 2011).

Si bien, las reformas legales son importantes a fin de que aquellos delitos descubiertos a través de un agente encubierto cibernético no queden impunes con el argumento de que para combatir la expansión de delitos en el espacio virtual en los que se pueden encontrar huellas digitales obtenidas sólo a través de mecanismos tecnológicos y no se pueda emplear la figura del agente encubierto. Herramientas cibernéticas como el agente encubierto en Internet, deben ser utilizadas por la fiscalía y la policía ya que los delitos son cibernéticos, y su entorno requiere de métodos específicos para la investigación criminal[20].

Tradicionalmente, se apunta que el libre acceso a los sitios en Internet ha facilitado la comisión de delitos tales como la pornografía infantil. No obstante, en la actualidad el uso de estos portales webs ha sido reducido, dado el constante monitoreo o patrullaje informático que realizan de forman conjunta cuerpos de seguridad y prevención de delitos.

En la constante lucha contra este flagelo se han utilizado mecanismos técnicos y tecnológicos con *softwares* o programas *RoundUp*, *Gridcopo Ephex*, para la geolocalización de las IPs que ayuden a identificar estas redes de intercambio de archivos perniciosos. Aunque se mantiene el intercambio de este material pornográfico a través de redes *peer to peer*[21], ya que solo se requiere acceder a la *Deep Web*[22] para estar fuera del alcance de la justicia. En este

excluidos del concepto de pornografía infantil los materiales que por su tosquedad revelen su condición de montaje" (Fiscalía General, 2015).

20 En este mismo sentido, citaremos la opinión de Bueno de Mata (2011), acerca de la figura del agente encubierto como una solución acertada en la lucha contra estas conductas criminales llevadas a cabo en Internet por estos criminales. "Depositando la fe en el buen hacer de las Fuerzas y Cuerpos de Seguridad del Estado, estamos seguro que en un tiempo no muy tardío se podrá lograr la justicia en el mundo del ciberespacio" (Bueno de Mata, 2011, p. 306).

21 "Las redes peer-to-peer (de igual a igual, de persona a persona), también conocidas como P2P, son plataformas que permiten el intercambio de archivos entre miles de usuarios conectados a Internet. A través de un programa informático específico de P2P, cada vez que el usuario accede a la red, comparte una carpeta de archivos con el resto de internautas conectados simultáneamente a una plataforma virtual, al mismo tiempo que puede acceder a los archivos compartidos por los demás internautas" (CEDRO, 2009, p. 22).

22 "Se conoce como Deep Web (también denominado Invisible Web, Hidden Web o Dark Web) o Internet profundo o invisible a todo el contenido que no forma parte del Internet superficial, es decir, de las páginas indexadas por las redes de los motores de búsqueda de la red. Esto se debe a las limitaciones que tienen las redes para acceder a todos los sitios web por distintos motivos. La Deep Web son los lugares en Internet donde los motores de búsqueda no pueden indexar: donde Google, Yahoo, Bing, etcétera no llega ni llegará. Por lo tanto, son "oscuros" y de acceso muy limitado. […] En el Internet profundo está alojado más del 80 por ciento del contenido real de Internet, se encuentra información clasificada, incluso páginas de carácter delictivo" (López-Barberá Martín, 2014, p. 96) El material consultado indica que no toda interacción en la Deep Web es de carácter delictual, puesto que se puede "encontrar con lo que llamaríamos "la parte buena" y el buen uso […] no deja de ser una herramienta al igual que la web normal) sino que depende del uso que se haga de ella y a qué niveles se acceda y para qué fin. - Nivel 0: Web común (buscadores tipo Google, Yahoo…). - Nivel 1: Encontraríamos bases de datos, información probada, direcciones... - Nivel 2: Aquí empezaríamos a hablar de páginas de carácter ilegal donde se encuentra pornografía o resultados de búsqueda bloqueada por otros servidores. - Nivel 3: Uso necesario de proxy. En este nivel se encuentran temas peligrosos que ya se encuadran dentro del cibercrimen. Desde pornografía infantil, grupos de intercambio de este tipo de materiales, virus... - Nivel 4: Los denominados 'onion'. Necesidad

sentido, se apunta que la persecución de las infracciones cometidas a través de estas redes y en esos niveles de la Web no resulta fácil:

> Se trata de actos llevados a cabo en una plataforma virtual a la que están conectados millones de usuarios, con el añadido de que los ficheros no se encuentran en un sitio web responsabilidad de un servidor, sino que están dispersos en los ordenadores particulares de los usuarios interconectados a través de un determinado programa (CEDRO, 2009, p. 22).

En estos escenarios surge la necesidad de instrumentar la actuación del agente encubierto cibernético, quien deberá utilizar anzuelos o trampas con la finalidad de pescar o atrapar a los delincuentes cibernéticos, estos instrumentos van más allá de las mentiras y engaños que habitualmente emplea el agente para infiltrarse, ya que en el circuito ciberdelictivo descrito, deberá aparentar ser un usuario poseedor de contenido relativo a pornografía infantil, cuyo intercambio le permitiría ganarse la confianza de los internautas pornógrafos o pedófilos "verdaderos"[23].

Resulta idóneo apuntar como ejemplo la modificación realizada en 2015 a la Ley española de Enjuiciamiento Criminal (BOE Nª 239, de 6 de octubre de 2015) a las facultades del agente encubierto, al tratarse de actuaciones informáticas contra pornografía infantil podrá:

> a) operar en el tráfico social, de los canales de comunicación cerrados, bajo una identidad ficticia, que esconda su condición de miembro de las Fuerzas y Cuerpos de Seguridad; b) intercambiar o enviar por sí mismo archivos ilícitos por razón de su cometido; c) analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos (Carou García, 2018, p. 28).

Como vemos se trata de un conjunto de actuaciones que podrá desplegar el agente para lograr hacerse del compañerismo y la camaradería de otros usuarios de estas redes delictivas con el fin de lograr su desmantelamiento y aprehensión, actuaciones que deberán estar precedidas por la autorización judicial, toda vez que estarían siendo vulnerados derechos fundamentales como el secreto de las comunicaciones, por mencionar alguno.

3.3. Elementos para la reforma legislativa

A los fines de asegurar una efectiva incorporación de la figura del agente encubierto cibernético en nuestro ordenamiento jurídico, planteamos dos elementos a considerar en la posible modificación legal.

El primer elemento corresponde al ámbito espacial donde se pueden realizar estas operaciones encubiertas, ya que como hemos anotado se trata de delitos que trascienden las fronteras y los límites nacionales, verificándose en la profundidad de la Web, que podría involucrar varios países. Si bien, es imposible que en el ordenamiento interno ecuatoriano se establezca la posibilidad de que los agentes policiales actúen por sí mismos en otro país, de

de utilizar Tor. Aquí se encuentra pornografía de cualquier tipo, asesinatos reales, imágenes de secuestros y torturas, tráfico de órganos, intercambio de divisas, hackers, documentos de anonymous (mediante Tor han organizado ataques masivos a todo tipo de organizaciones), tráfico de armas, intercambio de drogas, contratación de asesinos a sueldo, prostitutas, contactos de terrorismo y un largo etcétera que constituye el más largo mercado negro que se haya visto hasta ahora" (López-Barberá Martín, 2014, p. 97).

23 "El agente infiltrado opera en la Red bajo una identidad falsa, lo cual le permite adentrarse en los grupos cerrados de pedófilos, generando para ello una relación de confianza con alguno o algunos de sus miembros, que serán los que le proporcionen la indispensable invitación para formar parte de esas comunidades virtuales delictivas" (Carou García, 2018, p. 27).

la revisión realizada, nada impide que Ecuador se haga parte del Convenio de Budapest y/u de otros tratados que propugnan la cooperación y colaboración internacional en la puesta en marcha de operaciones encubiertas en Internet, donde intervienen cuerpos de seguridad de distintos países, lo cual conduce a una persecución internacional de estos delitos.

El segundo elemento se refiere a las facultades que se le deben dar al agente encubierto cibernético, que tal como ha sido referido por la doctrina, requerirá de ampliación de las formas tradicionales. A este respecto se requerirá modificar el contenido de los artículos 480 y 482 y del numeral 3 del artículo 484 del COIP referente al allanamiento y su procedimiento y a las reglas de las operaciones encubiertas, donde se establece que en ningún caso se permitirá al agente encubierto, impulsar delitos que no sean de iniciativa previa de los investigados. Esta modificación atenderá a la descrita necesidad de ganarse la confianza a través del intercambio de información en estas redes delictivas virtuales.

Las reformas descritas son importantes a fin de combatir la diversidad de delitos cibernéticos, los cuales son de imposible persecución en el limitado ámbito territorial de nuestro país, y donde las facultades para realizar operaciones encubiertas son también limitantes para los agentes.

4. Conclusiones

a. a. La urgente necesidad de generar cambios en los modelos de organización nacional e internacional por la proliferación de crímenes ocurridos en el ciberespacio, va dejando atrás aquella jurisdicción territorial que limita su efectiva persecución, a los fines de tener coherencia entre la lucha y lo que se desea lograr.

b. b. Alertar que en delitos tan atroces cometidos en el medio informático como los que tienen niños y niñas como víctimas, se constituyen temas de interés global, donde habría lugar a incorporar una excepción a la territorialidad, que de la mano de la cooperación internacional y la asistencia mutua en las investigaciones, aun entre países que no cuentan con tratados o acuerdos, toda vez que Internet no tiene fronteras ni conoce de jurisdicciones, permitan el intercambio continuo de información, así como a través de herramientas tecnológicas especificas, el monitorio constante de posibles sospechosos, a los fines de mitigar estos crímenes. Tal como apunta Sabrina B. Lamperti:

La cooperación oportuna y eficaz entre los países es fundamental para garantizar el éxito de una investigación porque, a diferencia de la investigación tradicional, es muy corto el tiempo de que dispone un investigador de delitos cibernéticos (Lamperti, 2014).

a. c. La existencia del Convenio de Budapest no hace invulnerable el ciberespacio ya que siempre surgirán novedosas situaciones que requerirán apelar a los principios de la cooperación internacional teniendo presente que en el ciberespacio a la hora de cometer delitos y de contrarrestarlos no hay límites territoriales o fronteras, los datos que se encuentran en las nubes de información son un claro ejemplo del tipo de problemas que surgen y para los cuales debemos estar cada vez más preparados.

b. d. Esa preparación pasa por ajustar operadores y funcionarios de justicia entre los que se encuentra el agente encubierto, al escenario virtual, donde su actuación no se puede limitar a un espacio finito, ya que el ciberespacio es infinito y las posibilidades de que las organizaciones criminales cometan actos contrarios a la ley socialmente reprobables, son igualmente infinitas.

Referencias bibliográficas

Albán, J. P. (2016). ¡Punir o no punir, esa es la cuestión! (el derecho penal ecuatoriano y la sociedad de la información). En *Regulación de Internet y derechos digitales en Ecuador*. Quito: Editorial USFQ.

Bueno de Mata, F. (2011). El Agente Encubierto en Internet: mentiras virtuales para alcanzar la justicia. En *Los retos del Poder Judicial ante la sociedad globalizada: Actas del IV Congreso Gallego de Derecho Procesal (I Internacional)*. A Coruña, 2 y 3 de junio.

Cano, J. (2007). Informáticos forenses: los criminalistas informáticos en la Sociedad de la Información. *Revista Derecho y Tecnología, Centro de Investigaciones Jurídicas y Políticas*, 9.

Carou, S. (2018). El Agente encubierto como instrumento de lucha contra la pornografía infantil en Internet. El Guardián al otro lado del espejo. *Cuadernos de la Guardia Civil,* 56, 23-40.

Castell, M. (2006). *La sociedad red: una visión global*. Madrid: Alianza Editorial.

CEDRO-Centro Español de Derechos Reprográficos (2009). Redes de intercambio de archivos P2P. *Boletín Informativo,* 68, 22-23. Recuperado de: http://www.cedro.org/docs/lecturas/bolequees68.pdf?Status=Master

Díaz Gómez, A. (2010). *El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest*. *REDUR* 8, 169-203.

Félix-Mateo, V. et.al. (2010) El ciberacoso en la enseñanza obligatoria. *Aula Abierta*, 38 (1), 47-58.

Gilles, P. (2017). Derechos Humanos y el Derecho Penal en el Ciberespacio. *Rev. secr. Trib. perm. Revis,* 5 (10), 274-286. https://doi.org/10.16890/rstpr.a5.n10.p274

Goodman M. (2003). *Cibercriminalidad*. Instituto Nacional de Ciencias Penales, Serie "Conferencias magistrales" 7: México.

Sain, G. (2018). Hacia una nueva ley de grooming. *Página 12*, 28 de marzo. Recuperado de: https://www.pagina12.com.ar/104365-hacia-una-nueva-ley-de-grooming

Lamperti, S. (2014). *Problemáticas en torno a la investigación de los delitos informáticos*. Congreso Iberoamericano de Investigadores y Docentes de Derecho e Informática CIIDDI Universidad FASTA Federación Iberoamericana de Asociaciones de Derecho e Informática, Sede: Mar del Plata. Recuperado de: https://www.researchgate.net/publication/324064192

López-Barberá, A. (2014). "Deep Web" o Internet profundo. *Seguritecnia,* 407, 96-97. Recuperado de: http://www.seguritecnia.es/revistas/seg/407/files/assets/basic-html/index.html#1

Molina, T. (2009). Técnicas especiales de investigación del delito: el agente provocador, el agente infiltrado y figuras afines (y II). *Anuario Jurídico y Económico Escurialense*, XLII, 153-174.

Riquert, M. (2017). *Delincuencia Informática: estándares internacionales para su tipificación y límites para su persecución*. Recuperado de: http://iccs.com.br/delincuencia-informatica-estandares-internacionales-pa

Legislación

Asamblea Nacional de la República del Ecuador (2014). *Código Orgánico Integral Penal*. Registro Oficial 180, 10 de Febrero de 2014.

Observaciones, Resoluciones, Recomendaciones, Informes y Opiniones Consultivas

Comisión de la Verdad. (2010). *Informe de la Comisión de la Verdad Ecuador 2010.* Recuperado de: http://repositorio.dpe.gob.ec/handle/39000/1312

Fiscalía General del Estado español. (2015). *Circular 2/2015, sobre los delitos de pornografía infantil tras la reforma operada por LO 1/2015*. Recuperado de: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Circular_2_15_pornografia_infantil.pdf?idFile=24b87ad2-9488-488a-ab0a-15d88e3048ed