EL PAPEL DE LAS POLITICAS PÚBLICAS Y LA NORMATIVIDAD EN LA PREVENCIÓN Y REGULACIÓN DEL CIBERDELITO

Autor: Harrysson Jahir Valderrama Estupiñan
Bogotá, 2018.

RESUMEN

En este artículo se hace una reflexión de los impactos generados por las políticas públicas nacionales y el desarrollo normativo nacional e internacional, en lo referente a la prevención y la regulación del Ciberdelito o delitos informáticos en la sociedad civil en Bogotá. Para esto se planteó dos puntos de desarrollo: 1) Muestra de resultados de un conjunto de encuestas a los directamente afectados por el ciberdelito y de unas entrevistas a expertos en el tema. 2) Discusión analítica sobre los posibles impactos de la norma y la política pública en las y los bogotanos. Estos dos puntos antecedidos por una descripción de las formas de ciberdelito en Colombia, así como de la regulación jurídica y de política pública, en lo relativo a los comportamientos que son vinculantes para los bogotanos dentro del ciberespacio.

Palabras clave: Ciberdelito, Políticas Públicas, Regulación Jurídica, Prevención, Bogotá.

ABSTRACT

In this article, a reflection is made of the impacts generated by national public policies and the national and international regulatory development, regarding the prevention and regulation of cybercrime or cybercrime in civil society in Bogotá. For this, two points of development were raised: 1) Sample of results of a set of surveys to those directly affected by the cybercrime and of some interviews to experts on the subject. 2) Analytical discussion about the possible impacts of the norm and public policy on Bogota citizens. These two points preceded by a description of the forms of cybercrime in Colombia, as well as legal regulation and public policy, regarding the behaviors that are binding for Bogota citizens in cyberspace.

Keywords: Ciberdelito, Public Policies, Legal Regulation, Prevention, Bogotá.

INTRODUCCIÓN

El presente trabajo es un artículo de investigación, que tiene como fin reflexionar sobre los posibles impactos de las políticas públicas nacionales y el desarrollo normativo, entorno a la prevención y regulación del Ciberdelito en la sociedad civil bogotana; haciendo hincapié en el análisis del entendimiento, valoración y actuación por parte de las y los ciudadanos en sus dinámicas cotidianas dentro del ciberespacio.

La intención de realizar este artículo, surge en primer lugar, de la obligación de dar respuesta al aumento de denuncias por delitos informáticos en Colombia, que según datos de la Fiscalía y la Policía crecieron en 31% en el 2017, y que para el mes de enero del 2018 presenta un incremento del 202% comparado con el mes del año anterior (El Tiempo, 2018). En segundo lugar, de la exigencia de hacer un análisis sobre los grandes costos económicos y culturales generados por los delitos informáticos o ciberdelitos en Colombia, puesto que según el periódico el (El Tiempo, 2016) los delitos informáticos para el 2015 generaron, a las y los colombianos una pérdida de 600 millones de dólares, y a esto se le suma los impactos sociales de estos delitos, a las personas en condición de vulnerabilidad como los menores de edad – Ciberacoso, Ciberbulling, pornografía infantil, etc…

Teniendo en cuenta las anteriores circunstancias, el artículo tiene como propósito principal generar una respuesta académica referente al entorno político y jurídico sobre los delitos informáticos como se tipifica en la normatividad nacional, y que generan expectativas, interrogantes e intrigas, en las y los ciudadanos sobre este nuevo delito, que aunque es actual ha desarrollado grandes impactos en las dinámicas de diario vivir de las y los bogotanos.

Con el fin de dar respuesta a los propósitos mencionados en los anteriores párrafos, este trabajo se plantea una pregunta central: ¿Cuáles son los impactos generados, por 1) las políticas públicas nacionales y 2) el desarrollo normativo nacional e internacional; en lo referente a la prevención y regulación del ciberdelito en la sociedad civil de Bogotá a partir del año 2006[1]? La cual tendrá tres partes que la responderán. Una primera parte que contempla la descripción de las formas de desarrollo del ciberdelito en Colombia; así como la descripción de las políticas públicas y la normatividad nacional e internacional de carácter vinculante que se ha

[1] Año a partir del cual entro en vigencia el documento CONPES 3854 de 2016 “Política Nacional de Seguridad Digital”, último documento de política pública desarrollado en Colombia.

desarrollado en Colombia entorno al Ciberdelito[2]. Una segunda parte que comprende la muestra de resultados de entrevistas y encuestas direccionadas al tema. Y por último una tercera parte concluyente en la cual se formula la discusión de las dos anteriores partes.

MARCO TEÓRICO

Formas de Ciberdelito en Colombia.

Antes de exponer las formas de ciberdelito que se dan en Colombia, hay que dar una idea general de lo que se entiende por ciberdelito desde el ámbito teórico. En este sentido desde la teoría, se destaca el recorrido teórico que hace el doctor en derecho Fernando Miró Llinares, y que llega a la conclusión que el ciberdelito desde los sentidos tipológico y normativo se concibe como

> un comportamiento concreto que reúne una serie de características criminológicas (también podrían ser legales) relacionadas con el ciberespacio (sentido tipológico), o para tratar de identificar un tipo penal concreto con un presupuesto y una sanción, que pretende prevenir la realización de conductas en el ciberespacio que afectan a bienes jurídicos dignos de protección (sentido normativo) (Miró Llinares, 2012, págs. 39, 40).

Desde otro sentido, el sentido epistemológico (también manejado por Miró Llinares), se dice que el termino cibercrimen[3] procede "de la unión entre el prefijo cyber, derivado del término cyberspace, y el término crime, como concepto que sirve para englobar la delincuencia en el espacio de comunicación abierta universal que es el ciberespacio" (Miró Llinares, 2012, pág. 37).

En conclusión en este artículo se tomara al ciberdelito como un conjunto de acciones u omisiones cometidas dentro del ciberespacio que promuevan un delito individual, social, económico, y/o político, contemplado en el orden jurídico territorial en el que se encuentre alguna de las partes implicadas (victima(s) y/o victimario(s)).

---

[2] Principalmente: "Convenio sobre Cibercrimenes" Budapest, 23 de noviembre de 2001; Ley 1273 de 2009; Documento CONPES 3701 de 2011 "Lineamientos de Políticas para Ciberseguridad y Ciberdefensa"; Documento CONPES 3854 de 2016 "Política Nacional de Seguridad Digital"; y en específico el Titulo VII BIS98 "De la Protección de la Información y de los Datos del Código Penal Colombiano".

[3] Entendiendo el cibercrimen como la aproximación general de los ciberdelitos.

Ahora bien, se va hacer un recorrido sobre cada uno de las formas de delitos informáticos que se llevan a cabo en Colombia y en el mundo; estas formas se condensan en tres grupos son: A. ciberdelitos o delitos informáticos con sentido económico, B. ciberdelitos o delitos informáticos sociales, y C. ciberdelitos políticos o ideológicos.

Ciberdelitos o Delitos Informáticos con Sentido Económico.

En este artículo se va entender los delitos informáticos económicos, como todos aquellos delitos informáticos que generen depreciaciones patrimoniales y demás costos económicos en los que tenga que incurrir un particular, una empresa o una sociedad comercial con ánimo o sin ánimo de lucro, por acciones informáticas intencionadas por parte de terceros.

Dentro de este tipo de ciberdelitos se pueden detectar tres modalidades, la primera de ellas de robo de información, la segunda de afectación del sistema, y la tercera de falsificación para transacciones.

En lo referente al robo de la información está el método Phishing que es el robo de la información con fines de estafa, este anterior en Colombia se presenta en dos formas como Smishing y como Vishing, y estos "corresponden a la difusión del mensaje y posterior llamada del delincuente, los premios por parte de operadores de telefonía celular y almacenes de cadena, la falsas ofertas en bolsas de empleo virtuales y la falsa llamada del sobrino retenido" (CCB, 2017, pág. 4).

Por otra parte la afectación o infestación del sistema, se refiere a la inserción maliciosa de virus a los diferentes sistemas, con el fin de generar estafa, entre las principales modalidades en Colombia se encuentra Malware, Ransomware, y por medio de las APT (Amenazas Persistentes Avanzadas).

Y por último están las falsificaciones para transacciones, que consisten en la falsificación de cuentas de e-mail, usuarios, paginas, etc… con el fin de realizar transacciones monetarias, su principal forma de expresión en Colombia es por medio de los BEC (Business Email Compromise) que se definen "como una estafa sofisticada, destinada a las empresas que trabajan con proveedores extranjeros y/o con empresas donde se llevan a cabo los pagos a

través de transferencias electrónicas internacionales" (CCB, 2017, pág. 6). Y que actúa través del fraude CEO, "en el que los ciberdelincuentes falsifican la dirección de correo ejecutivo de una organización, con el fin de iniciar una transferencia de fondos a sus propias cuentas" (CCB, 2017, pág. 6).

Otra forma de expresión de las falsificaciones para transacciones es el fraude electrónico en cajeros automáticos ATM, modalidad que se conoce como Skimming que consiste en que "los ciberdelincuentes logran hacerse de una copia de la banda magnética o chip correspondiente a una tarjeta de crédito o débito, la cual es utilizada para consumar un hecho delictivo, realizando compras o directamente retirando dinero de cuentas bancarias" (CCB, 2017, pág. 7).

Ciberdelitos o Delitos Informáticos Sociales

Este tipo de ciberdelito se refiere a todo ese conjunto de acciones que ocasionen perjuicios a la persona entorno a "su honor, intimidad, libertad sexual o similares bienes jurídicos" (CCB, 2017, pág. 2), dentro de este tipo se encuentran todos aquellos delitos propios del Ciberbullying[4] "Así mismo la instigación a delinquir, apología al delito, suplantación de identidad, sextorsión, grooming, entre otros comportamientos inaceptables" (CCB, 2017, pág. 8).

Este tipo de ciberdelito es la última evolución del mismo, puesto que este pasa de los daños que comprenden los delitos económicos, a daños propios de delitos a la persona (intimidad, buen nombre, libertad entorno a la expresión y el sostenimiento de actos sexuales, la dignidad, etc…) y además se expande en gran medida en un sector de la población vulnerable (los menores de edad), en palabras de Miró Llinares:

> […a..] partir del nuevo siglo empezaron a preocupar ya no sólo la información que pudieran contener los sistemas informáticos y la afectación a la intimidad o el patrimonio que pudiera derivarse del acceso a ella, sino el ciberespacio en el que los mismos interactuaban y los crímenes que allí se producían y que podían afectar a muchos otros nuevos bienes jurídicos como la indemnidad sexual, la dignidad (Miró Llinares, 2012, pág. 38).

[4] "en todas sus formas: burlas, ridiculización, intimidación, amenazas, extorsión, etc" (CCB, 2017, pág. 8).

Este delito informático ataca principalmente a la nueva generación (los Millennials), puesto que esta generación hace uso del ciberespacio para su comunicación, su trabajo, su establecimiento de relaciones etc…

Ciberdelitos Políticos o Ideológicos

Este tipo de ciberdelito hace referencia a esas acciones delictivas dentro del ciberespacio que perjudican el accionar y el libre funcionamiento de los Estados. Es decir estos delitos son

> cometidos con intención de desestabilizar un Estado o de difundir un determinado mensaje político aprovechando las posibilidades de comunicación masiva que ofrece el ciberespacio: la ciberguerra, el hacktivismo o el ciberterrorismo y que han convertido a los Estados, a los recursos públicos que ofrecen a los ciudadanos a través de Internet, en objetivo de ataques de denegación de servicio, de infecciones de malware u otros que pueden llegar, como ha sucedido, a paralizar la actividad de importantes instituciones de un país (CCB, 2017, pág. 2).

Desarrollo Normativo y de Política Pública sobre el Ciberdelito en Colombia

Dentro de la regulación normativa vigente sobre el tema, se encuentran en primer lugar los Artículos 15 y 20 de la Constitución Política de Colombia de 1991, que rezan respectivamente:

> **Artículo 15.** Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.
>
> En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.
>
> La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley.

> Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley.
>
> **Artículo 20.** Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación.
>
> Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura.

En segundo lugar, está la ley 1581 de 2012 que desarrolla los dos artículos anteriores:

> Articulo 1 La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

Por lo tanto esta ley tiene como objetivo regular todo lo correspondiente al suministro y el tratamiento de la información, así como los mecanismos de vigilancia y sanción de la misma y además se resalta que esta ley trae un componente de protección a la información de las niñas, los niños y los adolescentes (Artículo 7°. Derechos de los niños, niñas y adolescentes).

En tercer lugar está la ley 1273 de 2009: “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”; y que tipifica principalmente los siguientes delitos.

- Artículo 269A. Acceso abusivo a un sistema informático.
- Artículo 269B. Obstaculización ilegítima de sistema informático o red de telecomunicación.
- Artículo 269C. Interceptación de datos informáticos.
- Artículo 269D. Daño Informático.
- Artículo 269E. Uso de software malicioso.

- Artículo 269F. Violación de datos personales.
- Artículo 269G. Suplantación de sitios web para capturar datos personales.
- Artículo 269I. Hurto por medios informáticos y semejantes.
- Artículo 269J. Transferencia no consentida de activos.

Y en cuarto y último lugar, está la adhesión de Colombia en el 2004 del "Convenio sobre la Ciberdelincuencia" de Budapest, del 23 de noviembre de 2001; el cual trae como principal avance para Colombia, la definición de los siguientes delitos que atentan "contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informativos" (Convenio sobre la Ciberdelincuencia, 2001):

- Acceso ilícito.
- Interceptación ilícita.
- Interferencia en los datos.
- Interferencia en el sistema.
- Abuso de los dispositivos.
- Falsificación informática.
- Fraude informático.
- Delitos relacionados con la pornografía infantil.
- Delitos relacionados con infracciones de la propiedad intelectual y los derechos a fines.

Por otra parte, en lo concerniente al desarrollo de política pública, la primera política pública que se desarrolla entorno a los delitos informáticos en Colombia, es el CONPES 3701 de 2011 titulado "Lineamientos de política para Ciberseguridad y Ciberdefensa", cuyos objetivos principales son:

1. Implementar instancias apropiadas para prevenir, coordinar, atender, controlar, generar recomendaciones y regular los incidentes o emergencias cibernéticas para afrontar las amenazas y los riesgos que atentan contra la ciberseguridad y ciberdefensa nacional.
2. Brindar capacitación especializada en seguridad de la información y ampliar las líneas de investigación en ciberdefensa y ciberseguridad;[… y …]

3. Fortalecer la legislación en materia de ciberseguridad y ciberdefensa, la cooperación internacional y adelantar la adhesión de Colombia a los diferentes instrumentos internacionales en esta temática.

Dentro de sus mayores logros esta, la fuerte prevención y regulación en todo lo referente a los delitos informáticos políticos o ideológicos; y la creación y establecimiento de las siguientes dependencias:

- Grupo de respuesta a emergencias cibernéticas de Colombia (colCERT).
- El Centro Cibernético Policial (CCP) de la Policía Nacional de Colombia.
- El Equipo de respuesta a incidentes de seguridad informática de la Policía Nacional (CSIRT PONAL).
- La Delegatura de protección de datos en la Superintendencia de Industria y Comercio.
- La Subdirección técnica de seguridad y privacidad de tecnologías de información del Ministerio de Tecnologías de la Información y las Comunicaciones.
- El Comité de ciberdefensa de las Fuerzas Militares.
- Las Unidades cibernéticas del Ejército Nacional, la Armada Nacional y la Fuerza Aérea Colombiana.

La segunda y más ambiciosa política pública desarrollada en Colombia es el CONPES 3854 de 2016 y que se titula "Política Nacional de Seguridad Digital de Colombia", la cual se desarrollara hasta el año 2019 con una inversión total de 85.070 millones de pesos y cuyos principales objetivos son:

- Establecer un marco institucional claro en torno a la seguridad digital, basada en la gestión de riesgos.
- Crear las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital.
- Fortalecer la seguridad de los individuos y del Estado en el entorno digital, a nivel nacional y trasnacional, con un enfoque de gestión de riesgos.
- Fortalecer la defensa y soberanía nacional en el entorno digital con un enfoque de gestión de riesgos.

- Impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional.

METODOLOGÍA

Para realizar este artículo de investigación, se desarrollará una investigación reflexivo descriptiva sobre de la regulación normativa, de política pública en lo referente al tema del ciberdelito o delitos informáticos, y de recolección de opiniones sobre temas relacionados sobre este tópico.

La investigación se plantea bajo un carácter mixto, en tanto, incluye metodologías cualitativas y cuantitativas.

Parte cuantitativa: La muestra y descripción de los impactos por medio de las encuestas.

Parte cualitativa: La reflexión hecha sobre las opiniones recogidas por las entrevistas.

Muestra poblacional: La muestra poblacional por limitantes en recursos económicos y temporales será establecida a discreción del autor.

NOMBRE DADO AL GRUPO DE POBLACIÓN	CANTIDAD	MEDIO DE SUMINISTRO DE INFORMACIÓN
Ejecutores (Funcionarios públicos relacionados Centro Cibernético Policial)[5].	4	Encuesta
Teóricos (Abogados y Politólogos)[6]	4	Entrevista
Receptores 1 (Milennials)[7].	4	Encuesta
Receptores 2 (Usuarios frecuentes del ciberespacio)[8]	4	Encuesta

Para desarrollar lo anterior, se realizará lo siguiente:

1. La realización de entrevistas y encuestas a las personas directamente relacionadas con la regulación, y la prevención del ciberdelito.

[5] Funcionarios del Centro Cibernético de la Policía Nacional.
[6] Abogados especialistas en derecho Penal y politólogos especialistas en formulación, implementación y evaluación de políticas públicas.
[7] Toda personas aquella no mayor a 18 años y que depende en gran forma del espacio cibernético.
[8] Aquellos funcionarios de empresas privadas que usan con frecuencia las trasferencias digitales monetarias.

2. La realización de encuestas a las personas que se ven afectadas por el ciberdelito.
3. La revisión de normativa y de política pública como artículos de la Constitución, leyes, acuerdos internacionales y documentos CONPES.
4. Análisis entorno a los datos recolectados por las entrevistas y las encuestas realizadas.
5. Análisis completo de la normatividad investigada más las reflexiones que deje la discusión de las encuestas y las entrevistas.

Instrumentos a usar:

Acceso y Generación de Datos	• **Entrevistas semi-estructuradas** • **Corpus bibliográfico** • **Regulación normativa.** • **Documentos CONPES.**
Análisis de Datos	• Sistematización de datos en programas como Atlas.ti y SPSS • Análisis de contenido

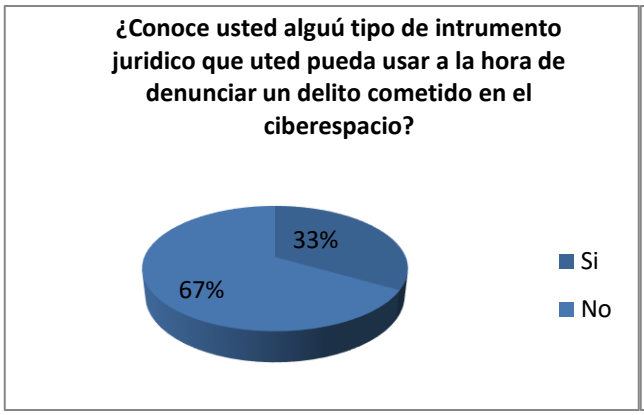
Cronograma:

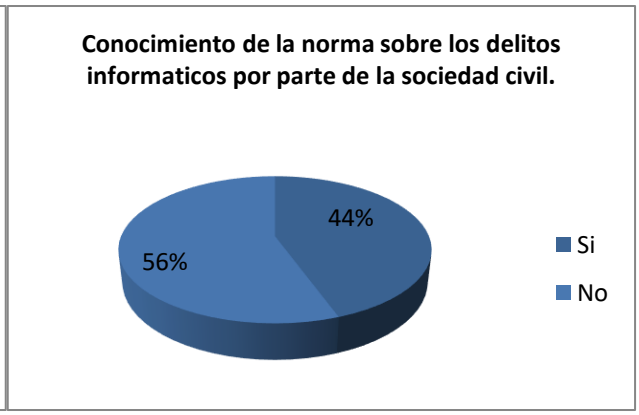
Tiempo de duración de la investigación					
Actividades a realizar	MARZO	ABRIL	MAYO	JUNIO	JULIO
Formulación de la pregunta-problema, justificación y objetivos del artículo.					
La revisión de normativa y de política pública como artículos de la Constitución, leyes, acuerdos internacionales y documentos CONPES.					
La realización de entrevistas y encuestas a las personas directamente relacionadas con la regulación, y la prevención del ciberdelito.					
La realización de encuestas a las personas que se ven afectadas por el ciberdelito.					

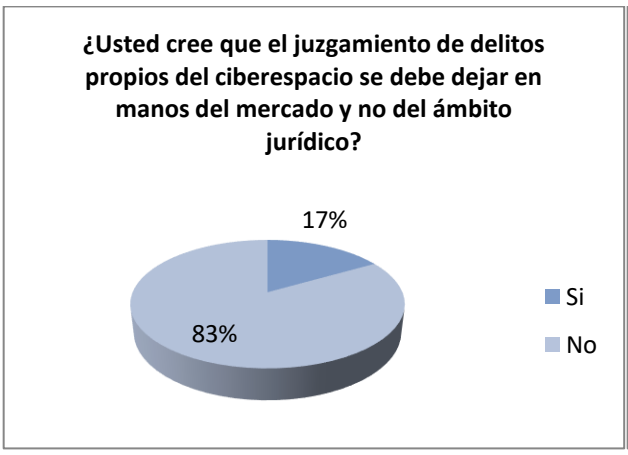
Descripción de los datos recolectados por las entrevistas y las encuestas realizadas.					
Reflexión de los impactos de la normatividad investigada más los datos y opiniones de las encuestas y las entrevistas.					
Publicación artículo.					

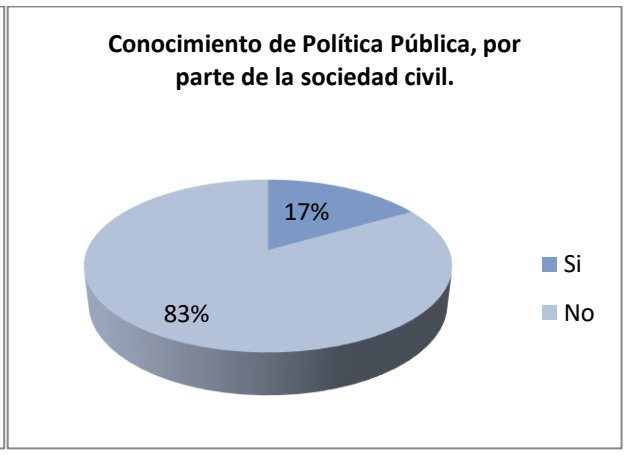
RESULTADOS

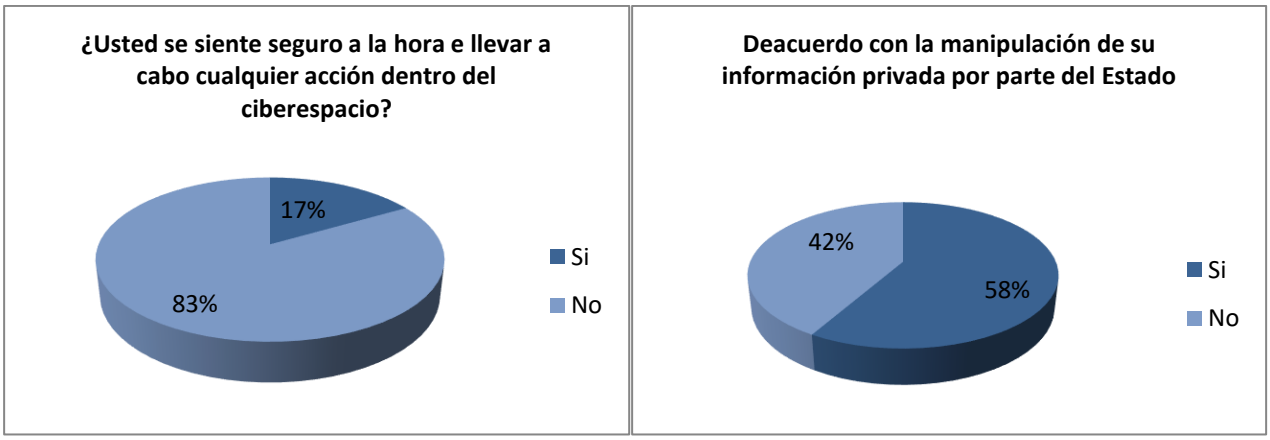
Resultados Encuestas

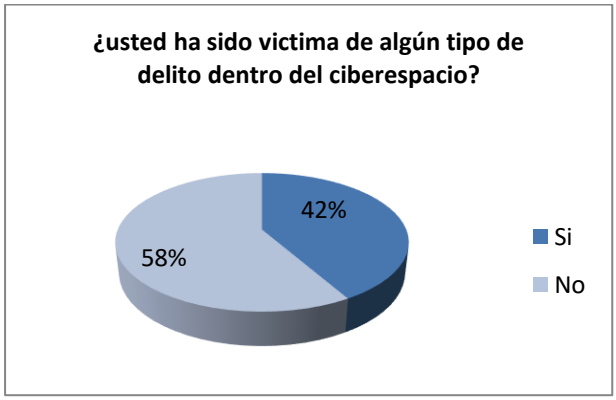












Resultados Entrevistas

En este apartado se expondrán las principales ideas, reflexiones y opiniones de los impactos implícitos de la normatividad y las políticas públicas sobre el ciberdelito en la sociedad civil bogotana, para esto se hará una exposición de las entrevistas realizadas al Magister en Políticas Públicas Sergio Andrés Martínez Silva, la Magister en Derecho Ivonne Patricia León, el Master jurídico en Derecho Internacional Camilo Elías Riaño Tovar y la Magister en Derecho Penal y Criminología Flor Alba Torres Rodríguez.

- Magister en Derecho Ivonne Patricia León

Pregunta: ¿Cuáles son los impactos de la política pública en la prevención y la regulación del ciberdelito en Bogotá?

Se parte de la idea que hay tres campos de influencia del ciberdelito: el global, el estatal y el local, todos estos interrelacionados. En el campo global se da una trasformación de las intercomunicaciones producto de la cuarta revolución tecnológica, que impulsa la digitalización

de la información y que permite nuevas amenazas relacionadas con el Internet y las redes de comunicación, amenazas que afectan directamente al segundo campo, es decir el estatal, que asumen principalmente dos clases de riesgos 1) el terrorismo, que viene de diversos actores (otros estados, organizaciones, civiles, etc…) y que implican el desarrollo de tecnologías militares que permitan la protección e información clasificada y de vital protección para los Estados y 2) el enfrentamiento de dinámicas que afectan de gran forma las economías estatales (como la injerencia de monedas ilegales, etc..). Estos riesgos llevan a que los Estados y a que el tercer campo, es decir las ciudades, en especial aquellas ciudades con aspiraciones globales como Bogotá, tomen acciones que apacigüen las fuertes efectos negativos de la comunicación global y sus riesgos.

Estas aspiraciones de ciudad Global se ven en el intento del distrito de fomentar por medio de políticas públicas 1) el mayor acceso gratis a internet, 2) el mayor uso de intercomunicaciones y 3) la transformación en una ciudad inteligente, políticas públicas que generan ciertas ventajas pero también grandes desventajas como:

- ✓ Un mayor control biopolitico por parte del Estado como del sector privado.
- ✓ Desaparición continúa del campo privado de las y los ciudadanos.
- ✓ Violación y apropiación de la información existente en el ciberespacio.
- ✓ La mayor dependencia de los servicios públicos a las conexiones en el ciberespacio.
- ✓ Desconfianza de las acciones y transacciones realizadas por las y los ciudadanos en el ciberespacio.
- ✓ Necesidad cada vez mayor por parte de las y los ciudadanos de vivir conectados.
- ✓ Aceptación con consentimiento pero sin entendimiento de todas las condiciones de uso legal del ciberespacio.
- ✓ Aumento de las políticas y dinámicas de ciberseguridad y ciberdefensa militar del Estado.
- ✓ Manipulación amplia de la información de las y los ciudadanos por parte del sector privado.
- ✓ El uso mayor del ciberespacio por parte de algunos sectores económicos ilegales, por su fácil evasión de la ley (narcotráfico, bacrim, etc…).

- ✓ Rezago de la normatividad vigente por parte de la evolución continúa de las formas de actuar del ciberdelito.
- Magister en Políticas Públicas Sergio Andrés Martínez Silva.

Pregunta: ¿Cuáles son los impactos de la política pública en la prevención y la regulación del ciberdelito en Bogotá?

Hay que partir de la diferenciación o tipología propia de las políticas públicas, es por esto que se parte de la idea que el delito en el sistema jurídico colombiano es entendido como una actividad que atañe única y exclusivamente al individuo, dejando a un lado las condiciones sociales y/o materiales que pueden llevar al individuo a cometer el delito; y es en este punto donde se puede empezar a diferenciar las políticas públicas, puesto que un primer tipo de políticas públicas no pueden desprender el delito de las causas materiales (la calidad de vida) como raíz del crimen, es decir estas políticas públicas que *se llamaran en este artículo* ***sociales*** (en tanto intentan dar mejoras sociales) parten de la idea que el origen del crimen es la necesidad y por lo tanto están orientadas a la búsqueda de condiciones aceptables de calidad de vida, lo que permitirá que en ultimas haya un mayor impacto en la disminución del crimen.

Hay un segundo tipo de políticas públicas *que en este artículo se llamaran* ***sancionatorias****,* que ante las falencias de las políticas públicas sociales, permiten la regulación y tipificación de los crímenes, en este sentido, el único fin de este tipo de políticas públicas es la represión por medio de las sanciones de conductas indebidas por parte de las y los ciudadanos.

No obstante los ciberdelitos no ocurren únicamente por cuenta de las necesidades materiales de las personas, ni tampoco se controlan por las medidas represivas y sancionatorias del sistema jurídico; el ciberdelito implica otro tipo de dinámicas (delitos sexuales, de relaciones sociales, de estrategia criminal[9], de carácter político, etc…), estas dinámicas son propias del ámbito privado de las personas, y es que donde surge el tercer tipo de política pública, *que en este artículo se llamaran* ***preventivas***, cuyo objetivo es la prevención, orientación y vigilancia por parte del Estado sobre los ciudadanos entorno a los riesgos propios del ciberespacio.

- Master jurídico en Derecho Internacional Camilo Elías Riaño Tovar

[9] Entiéndase por estrategia criminal, aquellas dinámicas propias de las organizaciones criminales, que hacen uso del ciberespacio, como dimensión en la cual a la legalidad le queda difícil su investigación y judicialización.

Pregunta: ¿Cuáles son los impactos del Derecho Internacional Público en la prevención y la regulación del ciberdelito en Bogotá?

El ciberdelito es un reto para el derecho internacional público, puesto que en un primer momento, hay varios convenios sobre el tema, pero estos que se enfocan en los derechos de autor y en la materia de la protección de documentos que tengan un componente electrónico, así como lo es el convenio de Budapest que hace énfasis en la definición del delito, quien se juzga y como se juzga. En un segundo momento el organismo especializado de las Naciones Unidas para las Tecnologías de la Información y la Comunicación UIT y las Naciones Unidas en la actualidad ante las acciones delictivas recientemente ocurridas (espionaje, inmunidad desde regímenes diplomáticos y la infracción de derechos de autor) intentan dar desarrollo entorno a la regulación del ciberdelito a nivel mundial.

- Magister en Derecho Penal y Criminología Flor Alba Torres Rodríguez

Pregunta: ¿Cuáles son los impactos de la norma en la prevención y la regulación del ciberdelito en Bogotá?

En la medida en que las personas van buscando medios para trasgredir las normas, que generan impactos negativos en la sociedad, la norma se emite para evitar los comportamientos que generan esas trasgresiones, y es esto a lo que se dedica el derecho penal. En este país se intenta solucionar todo por medio del derecho penal. Para esto se debe evaluar que debe o no incluirse dentro del derecho penal. Una vez que se evalúa que hace parte del derecho penal, es el legislador quien debe evaluar la sanción que se va a cometer por realizar ciertas conductas.

En el caso del ciberdelito hay unas personas que piensan como cometer unos comportamientos de forma diferente, evaluando como se infringe la norma, lo empiezan a hacer. Estos comportamientos generan grandes impactos en la sociedad, en el orden económico y en el Estado. En Colombia no hay prevención, porque no hay educación formal e informal, educación de valores a respetar los bienes de los demás, que tienen deberes, la prevención no es propia de la norma la debe hacer el Estado por medio de valores, la norma lo que hace es un contrarresto de la falta de valores de educación. La norma actúa únicamente como regulador, está es el control social secundario, es solo una respuesta a las falencias del control primario, es decir a las falencia del Estado.

DISCUSIÓN

Los resultados de las encuestas arrojan que el 67% de los encuestados no tienen conocimiento de herramientas jurídicas que pueden usar a la hora de ser víctimas de ciberdelitos; 56% de los mismos no tienen conocimiento sobre la normativa vigente sobre el ciberdellito; también un 83% desconoce la política pública que se ha desarrollado sobre el tema,; por otro lado solo un 17% de los entrevistados se siente seguro dentro del ciberespacio y un 42% ha sido víctima de ciberdelitos, además el 83% de estas personas considera que la regulación y la prevención de los ciberdelitos la debe realizar el Estado; y por último el 58% cree que el Estado debe manipular su información privada para así garantizar mayor seguridad.

De la entrevista al Magister Sergio Martínez se puede concluir que las políticas públicas sociales que intentan generar condiciones materiales a la población, generan desventajas, ante estas desventajas de las políticas públicas sociales, surgen las políticas públicas sancionatorias cuyo objetivo es fomentar medidas represivas y sancionatorias que regulen los crímenes producto de las desventajas de las políticas públicas. No obstante estos dos tipos de políticas públicas no exploran todas las dimensiones en las que se desarrolla el ciberdelito ni tampoco focalizan en el origen primario del ciberdelito, es decir el individuo, en este ámbito surgen las políticas públicas preventivas que actúan en cuanto a la prevención, orientación y vigilancia por parte del Estado sobre el individuo en el ciberespacio.

De la entrevista a la Magister Ivonne León se puede concluir que este conjunto de desventajas expuestas en la entrevista, han promovido acciones normativas de regulación por parte del Estado, en este sentido la norma se expide para solventar necesidades que generan las políticas públicas globalizantes del distrito, en tanto se convierten en un riesgo para el Estado.

De la entrevista al Magister Camilo Riaño se puede concluir que el ciberdelito es un reto para el Derecho Internacional Público, no obstante este es importante para los ciberdelitos que traspasan la jurisdicción nacional, pues estos solo pueden ser regulados en base al principio de subsidiaridad, y es en este punto donde el derecho internacional público entra a jugar, puesto que este es el único que mediante tratados, convenciones, acuerdos etc… puede generar normas y sanciones jurídicas comunes entre Estados que permitan la prevención, regulación y sanción

de los ciberdelitos, además es el derecho internacional público quien puede generar responsabilidad a alguna de las partes (es decir los Estados) y por último es el derecho internacional público quien regula todo lo relacionado con los tratados (celebración, nulidad y demás disposiciones) y son los tratados entre los Estados las fuentes principales de regulación existente sobre los ciberdelitos.

De la entrevista a la Magister Flor Alba Torres se puede concluir que dentro de la norma no hay prevención puesto que esta esta es el control social secundario, y al ser tal solo regula los comportamientos producto de las falencias del control social primario es decir las falencias del Estado, en este sentido se afirma que el ciberdelito al estar en constante avance no debe ser prevenido por la norma sino por el Estado a través de la educación y los valores que este infunde al núcleo familiar.

De lo anterior se pueden extraer dos grandes aseveraciones:

En primer lugar se evidencia como la población que se encuentra directamente y constantemente vinculada con el ciberespacio desconoce en gran medida la política pública y la norma que previenen y regulan los delitos dentro de este, así mismo también desconocen instrumentos que les permitan denunciar su calidad de victimas frente a estos delitos. En este sentido los objetivos de prevención propuestos en el COMPES 3854 del 2016 ha fallado en sus campañas de prevención de seguridad digital, en tanto sus programas de focalización no han llegado a brindar información a quienes más se ven involucrados con el ciberespacio *perse* quienes más necesitan información preventiva de seguridad digital, entendiendo así que aunque en Colombia si se ha desarrollado una política pública entorno al ciberdelito (es decir una política pública preventiva), esta no tiene mayor alcance y ha demostrado sus falencias en su implementación.

También se hace evidente el alejamiento de la norma de la realidad, puesto que el ciudadano desconoce los tipos de delitos de los que puede estar siendo víctima dentro del ciberespacio. Además se demuestra como los ciberdelitos al atravesar la jurisdicción de regulación de nuestro ordenamiento jurídico, deben necesariamente ser regulados por el Derecho Internacional Público, cuestión que como ya se dio a conocer es incipiente y obsoleta en Colombia, puesto

que nuestro único convenio vinculante es el de Budapest y este solo se encarga de definir los tipos de ciberdelito existente, dejando atrás la regulación de estos delitos.

En segundo lugar se puede evidenciar una sustancial percepción de inseguridad dentro del ciberespacio, así como gran parte de los entrevistados asimilan que es competencia del Estado la regulación y prevención de estos delitos y en este sentido se puede mezclar la percepción de inseguridad y la competencia del Estado para resolver esto, puesto que una parte mayor de estos considera que el Estado debe contar con información privada de sus ciudadanos para así garantizar una mayor seguridad dentro del ciberespacio.

En tercer lugar, dando así paso a que si bien el auge de una mayor exposición al ciberdelito, producto de las políticas públicas globalizantes de Bogotá, genera un desvanecimiento de la esfera de lo privado, es necesario su desmantelamiento de esta a favor del Estado, para que este último pueda garantizar seguridad. En este sentido la solución a las desventajas de la globalización de la ciudad (aumento de la inseguridad dentro del ciberespacio) es la profundización de estas en favor del Estado. Al igual la injerencia y competencia del Estado en cuanto la prevención de la norma es la ratificación de que es el Estado quien se debe encargar de la prevención del delito como control social primerio, y que además la norma solo debe actuar cuando el Estado haya sido incapaz de prevenir los delitos informáticos, por lo tanto solo debe regular ciertas conductas que actúan en contra del orden social.

Además se muestra como las cifras de la Fiscalía y la Policía pueden distar de la realidad en gran medida, puesto que como se mostró gran parte de los encuestados desconoce los instrumentos legales de defensa ante el ciberdelito, por lo tanto la mayoría de estos no usan la denuncia, es decir que si todas las personas que son víctimas de estos delitos realizaran sus respectivas denuncias, mostraría cifras alarmantes en Bogotá (puesto que es una ciudad enfrascada en gran forma en las dinámicas propias del ciberespacio)

CONCLUSION

En cuanto a la generación de impactos de la norma y la política pública en lo referente a la regulación y prevención de los ciberdelitos, se debe partir de una contextualización y un

relacionamiento, para así evidenciar los impactos. En primer lugar en cuanto contextualización se quiere dar cuenta que ese conjunto de normas y de políticas públicas actúan en una ciudad fuertemente influenciada y dirigida por políticas públicas globalizantes, que hacen que el ciberespacio se convierta en un ámbito importante de convivencia social, por lo tanto de necesidad de intervención del Estado, en este sentido se vuelve importante el papel que van a jugar las normas y las políticas públicas en esta intervención.

En segundo lugar, con respecto al relacionamiento se quiere dar cuanta del papel separado aunque complementario que tiene la política pública y la norma, entorno a la prevención y la regulación de los ciberdelitos. Teniendo en cuenta esto se parte de la idea, que es la política pública la que se debe dedicar a la prevención y esto en varios sentidos: a) Es la política pública la principal forma de acción del Estado, b) la articulación de las diferentes políticas públicas periten que ante falencias de unas políticas públicas (las sociales) se conformen otras políticas públicas de reacción elocuente (las regulativas) y unas más, de reacción trascendente (las preventivas), que en ultimas van a configurar el control al ciberdelito por medio de la prevención. Cuando la acción de prevención bajo política pública del Estado no tiene la capacidad de controlar el ciberdelito, es cuando entra la regulación del Estado, por medio de la norma; y su principal función es la de sancionar los actos ilícitos y no deseados que se cometen dentro del ciberespacio.

Con esta contextualización y relacionamiento ya se puede dar cabida a los impactos como tal.

Es así que se afirma, en primer lugar, que los mismos ciberdelitos son un efecto de las políticas públicas de carácter globalizante, así mismo la forma de reacción ante el auge de las ciberdelitos se da por medio de las políticas públicas preventivas, cuyos efectos no buscados son el acertamiento a la sociedad y el aumento de la percepción de inseguridad dentro del espacio y efectos buscados, como el desmantelamiento de la esfera privada del individuo por parte del Estado, así como la mayor injerencia del Estado en las dinámicas propias del ciberespacio. En segundo lugar, que los impactos de la norma son casi nulos, la norma solo tiene como objetivo, regular los ciberdelitos, y como estos están en constante y rápida evolución, las normas adquieren un carácter en gran parte obsoleto, además de esto y producto también de la evolución de los ciberdelitos, estas normas no son de conocimiento por parte de la población lo cual las hace más obsoletas.

Por ultimo haciendo un barrido de todo lo anterior, los efectos en cuanto a regulación y prevención, vienen principalmente de la política pública y de forma subsidiaria y en reducida parte de la norma, además son efectos en su mayoría negativos, que degradan las formas de inserción de las y los ciudadanos dentro del ciberespacio. Lo cual nos dejas varias preguntas ¿el control del ciberespacio debe ser únicamente por parte de política pública y de normas? Si es afirmativo ¿Se están aplicando los tipos de políticas públicas correctas? Y además ¿Es posible que los ciberdelitos sean un campo que permite dar cabida a nuevas formas de regulación y de formulación de políticas públicas?

REFERENCIAS

Código Penal, LEY 599 DE 2000 (Congreso de la República de Colombia 24 de Julio de 2000).

Ley 1273 de 2009 (Congreso de la República de Colombia 5 de Enero de 2009).

Documento CONPES 3701: LINEAMIENTOS DE POLÍTICAS PARA CIBERSEGURIDAD Y CIBERDEFENSA (CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL, REPÚBLICA DE COLOMBIA, DEPARTAMENTO NACIONAL DE PLANEACIÓN 2011).

Documento CONPES 3854: POLÍTICA NACIONAL DE SEGURIDAD DIGITAL (CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL, REPÚBLICA DE COLOMBIA, DEPARTAMENTO NACIONAL DE PLANEACIÓN 11 de Abril de 2016).

El Tiempo. (27 de Enero de 2016). Recuperado el 10 de Marzo de 2018, de http://www.eltiempo.com/archivo/documento/CMS-16493604

El Tiempo. (17 de Enero de 2018). Recuperado el 10 de Marzo de 2018, de http://www.eltiempo.com/justicia/delitos/denuncias-por-delitos-informaticos-crecieron-en-2017-172294

Gandini, I., Isaza, A., & Delgado , A. (5 de Enero de 2009). *Boletines DELTA*. Recuperado el 10 de Marzo de 2018, de www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia

Miró, F. (2012). El cibercrimen, Fenomenología y criminología de la delincuencia en el ciberespacio. Madrid. Editorial Marcial Pons.