BENEMÉRITA UNIVERSIDAD AUTÓNOMA DE PUEBLA

FACULTAD DE DERECHO Y CIENCIAS SOCIALES

SECRETARÍA DE INVESTIGACIÓN Y ESTUDIOS
DE POSGRADO

TESIS

LA INVESTIGACIÓN DE LA POLICÍA EN LOS CIBERDELITOS: UN ESTUDIO COMPARADO ENTRE MÉXICO Y ESPAÑA

TESIS PRESENTADA PARA OBTENER EL TÍTULO DE:
MAESTRÍA EN DERECHO

PRESENTA:
LIC. CITLALLI MUNGUÍA ZÚÑIGA

ASESOR:
DRA. ALICIA HERNÁNDEZ DE GANTE

DICIEMBRE DE 2014

BUAP

Oficio: SIEPD/726/2014
Asunto: El que se indica.

C.P JOSÉ JUAN MORALES RODRÍGUEZ.
DIRECTOR DE ADMINISTRACIÓN ESCOLAR DE LA B.U.A.P.
P R E S E N T E.

Muy distinguido Contador.

Por este conducto, nos permitimos distraer su atención para enviarle un respetuoso saludo y comunicarle lo siguiente:

Se ha designado como Jurado de Examen para obtener el *Grado Académico de Maestra en Derecho con terminal en Ciencias Penales de la* C.LIC. CITLALLI MUNGUÍA ZÚÑIGA el siguiente Sínodo:

DRA. ALICIA HERNÁNDEZ DE GANTE.....(PRESIDENTA)
DR. XAVIER NAJERA GONZÁLEZ.....(SECRETARIO)
DR. ALEX MUNGUIA SALAZAR.....(VOCAL 1)
DR. ALEJANDRO GALLARDO ARROYO.....(VOCAL 2)

El examen antes mencionado, se realizará el día 17 de Diciembre 2014 del año en curso, a las 13:00 hrs., en esta Unidad Académica.

Sin otro particular, reciba Usted atentos saludos.

A T E N T A M E N T E
"PENSAR BIEN PARA VIVIR MEJOR"
H. PUEBLA DE Z.A. 03 DE DICIEMBRE DE 2014.

DR. CARLOS ANTONIO MORENO SÁNCHEZ
DIRECTOR DE LA FACULTAD DE
DERECHO Y CIENCIAS SOCIALES

DR. FRANCISCO MARTÍNEZ ALPIZAR
SECRETARIO DE INVESTIGACIÓN
Y ESTUDIOS DE POSGRADO

c.c.p. Mtro. José Luis León Salamanca - Coordinador de Titulación y Egreso de la Facultad de Derecho.
c.c.p. Archivo.

Asunto: **Voto Aprobatorio**

Dr. Christian Federico Vargas García
Coordinador de la Maestría en Derecho
Facultad de Derecho y Ciencias Sociales
Benemérita Universidad Autónoma de Puebla
Presente

Muy estimado Dr.

Le saludo por este medio, al tiempo que hago de su conocimiento en calidad de directora del trabajo de tesis intitulado "La investigación de la policía en los ciberdelitos: un análisis comparativo entre México y España" que presenta la **Lic. Citlalli Munguía Zúñiga** para optar por el grado de Maestro en Derecho, que el mencionado trabajo de investigación ha sido concluido y revisado, por lo que pongo a su amable consideración lo siguiente:

La investigación realizada por la Lic. Munguía tiene como objeto de estudio la policía como una institución de servicio público en nuestro país que tiene la función de cumplir con las exigencias de proporcionar seguridad y custodia a la ciudadanía en general con prestación de eficacia y eficiencia en sus labores de investigación. Las instituciones de seguridad pública a cargo del Estado tienen la responsabilidad de mantener el orden público y la paz social ejerciendo su autoridad para el cumplimiento de leyes y reglamentos.

La aportación que realiza la Lic. Munguía en su investigación se relaciona con el desarrollo de las nuevas tecnologías de información que tiene impacto positivo en el progreso de las sociedades, pero también, con el uso indebido que se hace de ellas para cometer ilícitos.

Con estos presupuestos, enfoca su trabajo hacia lo que denomina los *ciberdelitos*, siendo propiamente su sujeto de estudio y analizando la problemática que se deriva de ellos.

Para tal efecto, parte con una conceptualización de la policía, concretándose en la policía cibernética creada en México en el año 2000 y analizando sus funciones en los delitos informáticos. Ello, necesariamente le lleva a investigar y analizar una serie de categorías nuevas en el Código Nacional de Procedimientos Penales aprobado en marzo de 2014, encontrando falta de tipificación de los *ciberdelitos*, falta de normatividad y el vacío de nuestras autoridades en la adhesión de México al Convenio de Budapest, instancia internacional que tiene entre otros objetivos, armonizar la legislación penal relacionada con el *cibercrimen*.

En este contexto, la Lic. Munguía realiza el planteamiento del problema desglosando una serie de condicionantes que urgen para México en cuanto a la normatividad, tipificación y capacitación de policías en una área penal tan especializada, propia de nuestro tiempo, y que desafortunadamente, va en aumento.

Para llegar a sus conclusiones y propuestas, la Lic. Munguía realizó un análisis comparativo con España, país que recién reformó su legislación sobre el tema, pero que muestra también, como México, el atraso en la regulación normativa de los *ciberdelitos*.

Por último, debo señalar que el tema de investigación es vigente y relevante obligando a la vez, a una exigente reflexión e importancia de nuevas áreas del derecho.

En atención a lo expuesto, y considerando que el trabajo de investigación cumple con las exigencias teóricas y metodologías del nivel de maestría, otorgo el **VOTO APROBATORIO** a la presente tesis a fin de que la Lic. Munguía continúe con los trámites académico-administrativos para la defensa de su trabajo ante el H. Sínodo.

Atentamente,
H. Puebla de Z., a 6 de noviembre de 2014

Dra. Alicia Hernández de Gante

A G R A D E C I M I E N T O S

A Dios, primero que nada y por sobre todas las cosas, por haberme regalado la vida y por darme el entendimiento para aceptar lo que no puedo cambiar y hacerme disfrutar de todo lo que puedo lograr.

A mis padres, porque no importa las veces que lo haya dicho, nunca será suficiente hacerles saber que los amo y que gracias a ellos soy lo que soy y por ello los honraré cada día que Dios me permita la vida.

A mis hermanos, Gigi, Ray y Cele, por todo el apoyo que siempre me han brindado, por el reconocimiento y confianza que me otorgan y a mis hermanas en especial por aquellos fines de semana en los que mientras yo leía las fuentes de consulta ellas escribían en la computadora.

A la ***Benemérita Universidad Autónoma de Puebla*** *y al* ***Consejo Nacional de Ciencia y Tecnología****, apreciables instituciones que me dieron la oportunidad y apoyo de llevar a cabo estos estudios y concluir este nivel académico.*

A la Doctora Alicia Hernández de Gante, tutora nacional, por su tolerancia, comprensión y nivel de exigencia, quien confió en mí siempre, bajo cualquier circunstancia.

Al Doctor Manuel Cancio Melía, tutor en el extranjero, por su enorme disposición y su gran sencillez para recibirme en otra Universidad y lograr hacerme sentir en casa. Con independencia de la gran admiración que le tengo.

A la Doctora Lizbeth Xóchitl Padilla Sanabria, asesora metodológica, por su atención y apoyo, quien cada semana mostró un interés en mi trabajo y gastó su valioso tiempo en revisarlo.

Al Abogado Guillermo España Irigoyen, porque ha sido para mí, un respetable líder, un gran jefe y un excelente amigo/hermano en todas las circunstancias que me permitieron obtener este logro.

A los Abogados José Salvador López Bribiesca y Alejandro Torres Madrid, porque sin su valioso apoyo seguro no hubiera llegado el día de ver cumplidos los objetivos.

A mis amigos (por orden alfabético) Abraham, Adry, Ángel, Angy, Atziri, Alejo, Beto, Carlos, Clau, Chio, Cony, Felipe, Donajhí, Hugo, Jaime, Jesús, Lupita, Lulú, Lluvia, Marco, Orlando, Rayito y Yair, a todos por su apoyo y a algunos especialmente por entender mi ausencia.

A ti JIRC, porque has llegado a darle a mi vida lo único que hace falta para convertirla en la vida como planeé que fuera, porque admiras lo que hago y lo disfrutas conmigo.

Dedico este trabajo a mis padres porque son el motor que mueve mi vida y a mis sobrinos: Fer, Isaac, Karlis, Esaú, Cami, Leo, Yael y Sam, quienes definitivamente fueron enviados por Dios a mi mundo para hacerlo aún más especial.

ÍNDICE

INTRODUCCIÓN

La sociedad evoluciona constantemente y a la par de esa evolución se van creando formas de cubrir las necesidades que demanda dicha sociedad, la invención y uso de nuevas tecnologías le permite al ser humano facilitar algunos procesos y con ello lograr tareas de manera breve que antes se realizaban en mayor tiempo. Sin embargo, no todos los individuos insertos en sociedad pugnan por la sana convivencia, ciertamente algunos son los que buscan de manera ventajosa un beneficio propio, echando mano del ingenio y creatividad que la tecnología les permite, se convierten en autores de hechos socialmente reprochables.

Así por ejemplo, llevan a cabo acciones que hace apenas unas décadas era imposible siquiera imaginar, o bien, innovan las formas de comisión de hechos comúnmente inadmisibles. Encontrándonos con la realización de conductas como aquellas que denigran la condición humana, viciándola y convirtiéndola en objeto de lucro o comercialización, por ejemplo, la pornografía infantil, la trata de personas y el turismo sexual, estos son algunos de los delitos, conocidos por todos, pero que con el surgimiento y difusión de lo que se conoce como informática, cada vez se hacen más frecuentes y fáciles de ejecutar al utilizar como medios comisivos el Internet y todas las funciones que de él deriven, convirtiéndolos así en delitos cometidos a través de medios informáticos o tecnológicos.

De tal suerte que cuando algún individuo o grupo de los que conforman la sociedad decide olvidar el beneficio común y utilizar las tecnologías para llevar a cabo delitos que lesionan más de un *bien jurídico* de la sociedad, el Estado debe intervenir a través de las Instituciones encargadas de la Seguridad Pública, su intervención debe ser acorde al *estado de Derecho* en el que vivimos; empero las Instituciones encargadas de la seguridad, se ven limitadas en sus funciones por múltiples razones.

En México, por principio de cuentas tenemos que las autoridades encargadas de perseguir los delitos, refiriéndome principalmente a la policía investigadora, se encuentra con la ausencia de tipificación en los catálogos penales de los delitos cometidos a través de los medios informáticos y todo lo que engloba el uso de las nuevas tecnologías, llámese ley adjetiva y sustantiva.

Por lo anterior y en virtud de habernos tocado vivir esta era de la tecnología en la que escuchamos por todas partes hablar de nuevos términos tales como *sociedad de la información*, *tecnologías de la información y comunicación, nueva era digital,* entre otras, nadie puede negar que la adopción de estos términos se debe a que la propia humanidad innovó su forma de vivir y creó instrumentos que le facilitaran su paso por este mundo y a la par se desarrollaron hechos en los que mediante la tecnología o valiéndose de ésta, se atenta en contra de la propia humanidad, conductas que por su naturaleza deben ser consideradas delitos.

No obstante, si dicha conducta no se encuentra descrita perfectamente en las leyes penales, hablemos de la ley sustantiva (Código Penal) y adjetiva (Código de Procedimientos Penales) tal como hoy ocurre en México, e incluso en muchas partes del mundo, entonces nos encontramos ante la necesidad de que el legislador observe la importancia que representa para la sociedad tener la seguridad de que cualquier hecho delictivo debe describirse perfectamente, para que pueda perseguirse y sancionarse y que para lograr el éxito en dichas acciones es necesario tipificarlo antes que nada, describirlo de manera clara y precisa, pues cuando ello no ocurre, nos encontramos con enormes lagunas que impiden una destacada participación por parte de las autoridades encargadas de brindar seguridad.

Ahora bien, si no existe una clara tipificación de los delitos llevados a cabo mediante el uso de la tecnología , podemos considerar una falta de tipificación de los *ciberdelitos* en México, la que trae consigo dificultades en contra de la investigación, ya que, mientras las instituciones intentan apenas adaptaahrse a las novedades, los grupos delictivos tienden a adaptarse rápidamente y aprovechar los

medios tecnológicos ampliando minuto a minuto su cobertura, lo que les da la oportunidad de no ser descubiertos o perseguidos y llevar a cabo con libertad conductas delictivas.

Como se ha mencionado, México y sus instituciones al servicio de la seguridad padecen la problemática, al igual que muchos otros países, sin embargo, la manera de asumir el compromiso para combatir estas nuevas conductas delictivas a estas situaciones ha de ser distinta en cada territorio del mundo, podrá depender de factores tales como legislaciones, instituciones y miembros de seguridad pública, los recursos económicos y tecnológicos con los que se cuente. No obstante, para poder determinar con precisión como hacer frente a estas situaciones en otras partes del mundo, en el presente trabajo de investigación se eligió a España, país miembro de la Unión Europea que ratificó en el año 2010 el Convenio del Consejo de Europa sobre el Cibercrimen y que por la estrecha relación histórica que guarda con México es motivo siempre de comparación, no obstante ser el único país de habla hispana en la Unión Europea.

De esta forma el objeto de estudio del presente trabajo de investigación lo constituye la policía, vista como una institución de servicio público, cuyo principal objetivo es satisfacer las necesidades de los gobernados en cuanto a la custodia y seguridad, empero, mediante un servicio de investigación eficiente y eficaz. Ciertamente ante la falta de tipificación de algunas conductas, la institución a que nos referimos se ve limitada en sus funciones y, para efectos de esta investigación, lo que denominamos *ciberdelitos* se convierte en el sujeto de estudio, siendo necesario llevar a cabo un análisis de la problemática que representa la existencia de estas conductas.

El objetivo general de esta investigación es demostrar que la ausencia de tipificación de los *ciberdelitos* en México es una limitante en el eficaz desempeño de la función de la policía investigadora, en relación con el tratamiento que se le da a la investigación de estos delitos en España. Esto sólo podrá realizarse gracias al

desarrollo de cuatro objetivos particulares mismos que guardan estrecha relación con los capítulos que integran este trabajo, a saber:

En el primer capítulo el cual se denomina *DE LA POLICÍA,* se pretende presentar de manera breve la evolución de lo que ha sido la policía en México, desde sus orígenes y hasta la actualidad, pasando a través de las épocas históricas que han marcado el desarrollo de este país, con la finalidad de presentar generalidades de los antecedentes de la policía como institución de seguridad pública, y así aspirar a llegar al análisis de la actual *policía cibernética*, desde su creación y las causas que la motivaron hasta las funciones que hoy día realiza.

El segundo capítulo llamado *DE LOS DELITOS CIBERNÉTICOS, INFORMÁTICOS O CIBERDELITOS,* fue realizado con la finalidad de dar a conocer de manera general aquellos conceptos utilizados y reproducidos en las actividades que, mediante el uso de la tecnología, conllevan un carácter delictivo. Dando pauta al análisis de los *ciberdelitos*, desde una perspectiva teórico-jurídica intentando llegar a la construcción propiamente del significado de lo que para la autora de esta investigación tendría que ser llamando *ciberdelito*, la clasificación que se ha realizado al respecto, ya sea aportada por expertos o bien, por Organismos Internacionales, inclusive los varios elementos que han surgido en pro de combatirlos, lo anterior con la finalidad de mostrar la gran importancia que ha adquirido en todo el mundo el surgimiento de estas nuevas conductas.

En el tercer capítulo que se titula *DE LA INVESTIGACIÓN DE LA POLICÍA EN LOS DENOMINADOS CIBERDELITOS,* se pretende llevar a cabo un estudio de la actuación de las autoridades investigadoras de los *ciberdelitos* en México, pasando por todos aquellos factores que propician dicha investigación, esto es el análisis al origen de las conductas que llegan a convertirse en delitos y por tanto un indispensable estudio a la legislación mexicana que de la materia existe a fin de hallar las limitaciones o bien, determinar los aciertos durante el ejercicio de la función investigativa que realizan las autoridades.

El cuarto y último capítulo de esta investigación, *LA INVESTIGACIÓN DE LOS CIBERDELITOS: ESPAÑA,* está dedicado al análisis de la actuación que tienen las autoridades investigadoras españolas, análisis que también se enfocará a la legislación de ese país respecto de los *ciberdelitos*, pretendiendo mostrar si la tipificación en el nuevo Código Penal de 1995, ha ayudado a que la investigación de la policía y en general el combate a la *ciberdelincuencia* se eficaz y cómo ha resultado el uso de las técnicas de investigación vinculadas a las nuevas tecnologías en favor de la justicia, así como señalar si en realidad existe una superioridad significativa en la investigación por parte de las autoridades españolas para hacer frente a la *ciberdelincuencia,* respecto del tratamiento que se le da a estas conductas en México.

Finalmente, hemos de llegar al apartado donde se advierten las doce conclusiones a las que la autora de esta investigación ha llegado, luego del estudio realizado en los cuatro capítulos que componen la investigación, así también se encuentra la propuesta que se presenta en este trabajo investigativo, la que se divide en tres etapas, la primera relativa a la tipificación de los ciberdelitos y la segunda y tercera a un modelo único de policía cibernética cuyos miembros cumplan con el perfil adecuado.

Lo anterior a fin de comprobar la hipótesis que se ha planteado en esta investigación y misma que se refiere a que *la adecuada tipificación de los ciberdelitos en México, hará que la investigación de la policía, resulte altamente eficaz.*

Para la realización de este trabajo, fueron utilizados métodos teóricos de investigación, como lo es el histórico-lógico, inductivo-deductivo y análisis-síntesis, además de la técnica de investigación documental, técnica que fue aplicada en los Países de México y España, gracias a que fui aceptada para realizar una estancia

corta de investigación en la Universidad Autónoma de Madrid de España y con ello tuve acceso a la biblioteca de la Facultad de Derecho de esa Universidad.

AREVIATURAS Y SIGLAS

AFI	Agencia Federal de Investigación
AMIPCI	Asociación Mexicana de Internet
BOE	Boletín Oficial del Estado (España)
CDPC	*European Committe on Crime Problems* (Comité Europeo sobre Problemas de Delincuencia)
CERT´s	Centros de Respuesta a Emergencias de Cómputo (también llamado CERT cuando se habla en singular)
Cfr.	Confróntese
CISEN	Centro de Investigación y Seguridad Nacional
CP	Código Penal
DOF	Diario Oficial de la Federación
FGE	Fiscalía General del Estado
Ibidem	En el mismo lugar
Idem	Igual
INTERPOL	La palabra es una contradicción de la expresión inglesa *international police* (policía internacional)
IP	Protocolo Internet
ISP	*Internet Service Provider* (Proveedor de Servicio de Internet)
LECrim	Ley de Enjuiciamiento Criminal (España)
LGT	Ley General de Telecomunicaciones (España)
LOPJ	Ley Orgánica del Poder Judicial
LORTAD	Ley Orgánica de Protección del Tratamiento Automatizado de los Datos de Carácter Personal (España)
MP	Ministerio Público
OCDE	Organización para la Cooperación y Desarrollo Económicos
OEA	Organización de Estados Americanos
ONU	Organización de las Naciones Unidas
Op. cit.	Obra citada
PFP	Policía Federal Preventiva
SCJN	Suprema Corte de Justicia de la Nación
s.e	sin editorial
TCP	Protocolo de Transmisión de Control
TDH	Tribunal Europeo de Derechos Humanos
Tic (tic´s)	Tecnologías de la información y comunicaciones (en ocasiones también se le llama tic´s, término adoptado en el ámbito gubernamental)
UIT	Unión Internacional de Comunicaciones

CAPÍTULO 1. DE LA POLICÍA

1.1. Concepto

Es menester dar inicio a la presente investigación, conceptualizando, por principio de cuentas, el objeto de estudio de que se tratará la misma, dicho lo cual, considérese entonces al autor Gerónimo Miguel Andrés Martínez, quien retoma del Diccionario Jurídico Mexicano, el concepto de *policía*, elaborado por Héctor Fix Zamudio, y que al juicio de la autora de esta investigación, podrá ser uno de los más completos:

> I. (Del latín *politia*, organización política, administración, que a su vez proviene del griego politeia, perteneciente al gobierno de la ciudad.) Aun cuando la voz policía puede entenderse también como lineamientos de la actividad política de acuerdo con su acepción original, en el ordenamiento mexicano, su sentido propio corresponde a la de los cuerpos de seguridad pública encargados de la prevención e investigación de los delitos y faltas, en auxilio del Ministerio Público (MP) y de los tribunales judiciales.[1]

En ese mismo orden de ideas, obsérvese como define el concepto el Diccionario Esencial de la Lengua Española, dividiéndolo en tres acepciones distintas, que pueden en determinado momento ser el complemento una de la otra para crear un concepto más elaborado; dicho concepto ha sido retomado por Octavio A. Orellana Wiarco, de la siguiente manera:

> Cuerpo encargado de velar por el mantenimiento del orden público, y la seguridad de los ciudadanos, a las órdenes de las autoridades políticas.
> Buen orden que se observa y guarda en las ciudades y repúblicas; cumpliéndose las leyes u ordenanzas establecidas para su mejor gobierno.

[1] Andrés Martínez, Gerónimo Miguel, *Derecho de policía (policiología y seguridad pública),* México, Flores Editor y Distribuidor, 2010, p.133.

> Cada uno de los miembros del cuerpo encargado de velar por el mantenimiento del orden público.[2]

De lo anterior se advierte, que pueden hallarse dos puntos de vista, el primero que tiene que ver con la institución, es decir, como cuerpo policial, integrado por el conjunto de mecanismos que se organizan en torno a un sistema, cuya esencia se encuentra en el poder público del Estado, en la prevención y la represión de conductas antisociales, sean estas infracciones administrativas o aun delitos; y el segundo que se refiere a la actividad desplegada para llevar a cabo el ejercicio de ese poder público.

Finalmente y no como concepto, sino más bien como una apreciación, reproduciendo la idea de Jesús Martínez Garnelo, tenemos que:

> La policía, en términos generales, es una institución de servicio público cuyo propósito es satisfacer las necesidades de la comunidad en cuanto a su custodia, seguridad, pero sobre todo, por medio de un servicio de investigación de eficacia y eficiencia.[3]

1.1.1. Etimología

Para entender el concepto de policía, es necesario conocer el significado de la palabra *policía*, tenemos que etimológicamente viene del latín *politia* que equivale a política o administración gubernativa. También se deriva del griego *politeia*, que pertenece al gobierno de la ciudad y de acuerdo a estas raíces entendamos la palabra policía como cuerpo creado para mantener el orden público.[4]

---

[2] Orellana Wiarco, Octavio A., *Seguridad pública, profesionalización de los policías,* México, Porrúa, 2010, p. 72.

[3] Martínez Garnelo, Jesús, *Sistema Nacional de Seguridad Pública,* 2ª ed., México, Porrúa, 2012, p.319.

[4] Ramírez Ramírez, Efrén, *La ética en la formación de la policía, manual de capacitación,* México, Porrúa, 2009, p. 111.

Ahora bien, póngase atención a este otro concepto en el que Bernardo Gómez del Campo Díaz Barreiro también señala que *policía*: "De manera indirecta deriva del latín *politia,* y del griego ciudad, que se refiere al gobierno o a la administración del Estado".[5] No es óbice mencionar que gran parte de los conceptos utilizados hoy en día, señalan que el uso de la palabra *policía* data de la etapa antigua de la civilización.

De lo anterior advertimos entonces, que es necesario considerar en sus orígenes a la *policía,* como la encargada de la administración del Estado, con ese fin surge y el éxito de su permanencia se debe al objetivo de mantener el orden en el mismo. Dicho lo anterior y por deducción, quien pertenezca, forme parte o se integre al cuerpo creado para mantener el orden público es un policía.

Puesto que el término *policía* se aplicaba a toda actividad administrativa, veamos desde dicha perspectiva que es "Aquella actividad que la administración pública despliega en el ejercicio de sus propias potestades, que, para garantizar el mantenimiento del orden público, limita los derechos de los administradores mediante el ejercicio, en su caso, de la coacción sobre los mismos".[6]

Cabe destacar que para la finalidad administrativa, a la policía se le ha de dar un tratamiento como mera actividad, cuyo ejercicio va encaminado a la administración pública que corre a cargo del Estado.

1.2. Breve reseña de la Policía en México

1.2.1. México Prehispánico

Para todos es indiscutible que durante la época prehispánica, hubo culturas que destacaron en muchos ámbitos de su organización, por hacer mención, la

[5] Gómez del Campo Díaz Barreiro, Bernardo, *En búsqueda de un perfil policial mexicano,* México, Porrúa, 2010, p. 1.

[6] Torres Bravo, Sergio Ibán, *Perspectiva general de la seguridad pública,* México, s.e., 2013, p. 69.

cultura maya, texcocana y azteca, las que precisamente alcanzaron un alto grado de desarrollo en el tema de procuración de justicia, por ende en sus sistemas de policía y seguridad.[7] Bernardo Gómez del Campo Díaz Barreiro habla al respecto del pueblo maya:

> El Derecho Penal Maya era riguroso, con penas severas que iban más allá de la reparación del daño, hablamos de esclavitud, repudio, vejación, mutilación, crueldad y hasta la pena de muerte. Son notables los delitos de traición contra el señor; las ofensas al grupo social, el homicidio, el hurto, las deudas, el incendio, la ebriedad, el adulterio, la violación, la prostitución; clasificando los delitos en intencionales y sin intención. Se auxiliaban de grandes jaulas de madera destinadas al encierro de criminales hasta su ejecución.[8]

Por otra parte el pueblo Texcocano, en materia de administración de justicia comparte algunos rasgos característicos con los de los tribunales aztecas, a decir de Jesús Martínez Garnelo, el derecho alcanzó el mayor auge de entre todos los pueblos autóctonos de ese tiempo y citando a Pomar señala:

> En aquellos días en la cultura texcocana tenía el rey su audiencia real, donde oían de justicia, ciertos hombres para ello señalados y escogidísimos en discreción, habilidad y buena conciencia, oían y conocían de las causas civiles y criminales que se ofrecían entre todo género de partes, de cualquier calidad que fuesen y sentenciaban conforme a las leyes. Las cosas arduas las comunicaban al rey, y las dudosas, se las remitían, y él los determinaba, después de muy bien informado de los jueces que llamaban Tetecuhtiu, y de las propias partes. Había de estos seis de sangre real y otros tantos de los plebeyos, personas de mucha prueba y larga experiencia.[9]

En ese mismo orden de ideas y siguiendo con Jesús Martínez Garnelo, quien ahora cita a Motolinía, nos indica que en Texcoco había jueces exclusivamente

---

[7] Ramírez Ramírez, Efrén, *op., cit*., nota 4, p. 115.
[8] Gómez del Campo Díaz Barreiro, Bernardo, *op., cit.,* nota 5, p. 3.
[9] *Ibidem,* p. 36.

dedicados a canalizar en procesos, las dificultades derivadas de los divorcios y matrimonios. Cada juez llamado Tecuytlatoque, ordenaba a un alguacil mayor ejecutor Achcautli, que aprehendiera aun a las personalidades destacadas que resultaban culpables en el juicio. [10]

Como se observa, los primeros indicios de las facultades otorgadas a la policía se pueden hacer manifiestas en los *Achcautli*, que cumplían una orden de aprehensión externada por un Juez, justo como hoy día se ejecuta; lo que nos muestra que las naciones deben ajustar su estructura y su organización a sus propias necesidades, sin imitar a otras naciones o aplicar otros modelos, tal como lo hicieron antaño y se conserva en esencia.

Por cuanto hace a la cultura Azteca, la forma de organización fue similar a la Texcocana, se multiplicaron las funciones administrativas surgiendo, lo que ya era posible denominar, un servicio policial, conformado por los Achcauhtli, aquí también auxiliares de los jueces, quienes además efectuaban detenciones de los criminales, hacían cumplir los fallos del tribunal y ejecutaban sentencias de muerte. Este tema es abordado a mayor profundidad por Bernardo Gómez del Campo Díaz Barreiro, quien señala:

> Los Topili, por su parte, eran auxiliares de los Achcauhtli, y llevaban a cabo la función persecutoria, aprehendían a los delincuentes y actuaban en ocasiones como verdugos. Adicional a lo anterior, existía la figura del Tlayacanqui, tenientes que auxiliaban a los jueces en la captura de los delincuentes y en la ejecución de las sentencias. Los Centeclapixque que realizaban funciones de policías, y eran electos directamente por los vecinos para permanecer por un año en sus cargos. Los Calmimilocatl que estaban responsabilizados de la vigilancia de cajas y tránsito de las canoas. Los Tianquizpan y los Tlayaque, mantenían el orden en los mercados y tianguis, y los Acolnahuacatl responsables de los islotes y chinampa. Otras personas que realizaron funciones de índole policial fueron los guardianes de los templos,

[10] Martínez Garnelo, Jesús, *La policía nacional investigadora del delito,* México, Porrúa, 1999, p. 34.

cárceles y escuelas, protectores de los comerciantes y de las riquezas que pagaban los pueblos dominados.[11]

Otros de los aspectos de suma importancia dentro de la organización de los aztecas y que prevalece al día de hoy, fueron las funciones preventivas, mismas que corría a cargo de un grupo denominado *contempopixquex,* éstos cuidaban el orden y vigilaban como medida de seguridad a aquellos sujetos de los cuales se tenían conocimientos de antecedentes criminales o mala conducta.[12]

Podemos subrayar que el servicio policial de las tres culturas más destacadas del México prehispánico, comparte similitudes, como se ha visto, incluso existen las mismas figuras, tal es el caso de los Achcauhtli, que para los aztecas y texcocanos, tendrían a cargo la función persecutoria, no obstante, la figura que más se asemeja a lo que hoy conocemos como policía preventiva son los *contempopixquex*, avanzada y sumamente precisa para su época.

1.2.2. La Colonia

A la caída de Tenochtitlan una nueva cultura se impone principalmente con una nueva lengua y una nueva religión, con sus tradiciones y su derecho, un nuevo dominio que se extiende desde Centroamérica, hasta límites con Canadá. En efecto habían llegado los españoles y con ellos toda un regeneración de las estructuras organizacionales, como se conocieron durante la época prehispánica.[13]

La invasión de una nueva cultura que sometió al pueblo y lo obligó a adoptar nuevas reglas y dejar a un lado los sistemas de justicia que se habían creado y el Derecho que se había construido, para dar paso a una época de sometimiento e imposición de normas que inconvenientemente los españoles traían consigo y que perdurarían durante los tres siglos que duró el colonialismo.

---

[11] Gómez del Campo Díaz Barreiro, Bernardo, *op., cit.,* nota 5, *p*. 3.
[12] Andrés Martínez, Gerónimo Miguel, *op., cit.,* nota 1, p. 16.
[13] Ramírez Ramírez, Efrén, *op., cit*., nota 4, p. 117.

En la época colonial, con la conquista española, se trasladaron a sus colonias, relaciones de producción y sistemas de dominio feudales y dentro de ellos, la función policial que tenía como objetivo cuidar el orden social existente y los intereses del Estado Español. Los Alguaciles Mayores y Teniente Alguacil, que aparecen, cuando Hernán Cortés organizó el Ayuntamiento de la Villa Rica de la Veracruz, se les otorgó función policial. Estos funcionarios auxiliaban a los Alcaldes Mayores en la aplicación de las penas severas para acabar con ladrones y mal vivientes que plagaban las ciudades y los caminos, así como la aprehensión de los delincuentes. Por otra parte, los Alguaciles Menores, nombrados por los Alguaciles Mayores, ayudaban a estos en la ronda y el patrullaje para aprehender a los delincuentes en flagrancia; podían ser de ciudad o de campo, según su competencia y decomisaban armas a personas que las llevaran de noche, excepto si portaban linternas o madrugaban para ir a trabajar. Existe otro tipo de alguaciles como los de los indios, que buscaba incorporarlo al sistema español, cuidar de su seguridad y buscar que llevara maíz a sus depósitos así como velar por el orden general entre ellos. El alguacil de doctrina vigilaba la impartición de la religión católica a los indios; por su parte los Alguaciles del crimen, vigilaban la práctica de las buenas costumbres para terminar con el vicio del juego, rondar calles obscuras y estar pendientes de las pulquerías. Los Alguaciles del Consulado que vigilaban embarques recogían mercancías en caso de naufragio o avería y detenían comerciantes defraudadores y los Alguaciles Mayores del Santo Oficio, que se encargaban de capturar a los responsables de herejía. Otros encargados de la seguridad pública eran los Fieles ejecutores, que vigilaban los mercados. Los Diputados de Policía encargados de hacer cumplir los bandos. Guardias Almóndigo y Pósito, custodios de almacenes públicos. Soldados de Presido, organizados en 1659 como vigilantes de las prisiones. Ministros Inferiores, que en 1664 fungieron como inspectores de ingesta de alcohol. Ministro de Vara y Ronda (1734) encargados de los seis cuarteles en los que se dividió la ciudad con funciones de índole policial. Alcaldes de Barrio o cuartel, que en 1782, estuvieron al frente de ocho cuarteles mayores y 32 de acuerdo a la división de la propia Ciudad. Alcaldes de corte (1778) encargados de penas de muerte o mutilación. Vigilantes de Plaza de Armas y Policías de Seguridad y Ornato para garantizar la paz, la tranquilidad y cuidar el aspecto de la capital novo hispana. Finalmente los más representativos, Vigilantes Nocturnos conocidos como

> Guardafaroles y Serenos, que, en su conformación, 1790, tenían como obligación pasarse la palabra unos a otros desde las once de la noche diciendo la hora y la situación que se presentaba cada 15 minutos. El silbato que llevaban lo usaban en caso de peligro.[14]

Ahora bien, para este momento, como es posible apreciar, se había hecho adoptar la forma de organización policial que los españoles impusieron, por tanto se aprecia entonces que para cada actividad del Estado, había detrás una figura policial encargada de hacer cumplir las finalidades para las que estaba encargado, así pues había cualquier cantidad y diversas clases de policías, algunos de los cuales, prevalecen en la actualidad incluso con indicios del mismo nombre.

Bajo el mismo contexto, José Arturo Yañez Romero, hace un análisis de los alcaldes de barrio, figura que cobraría su importancia a fines del siglo XVIII, tales no tenían propiamente competencia judicial más que integrar la instrucción sumaria de los delitos, pero desde el punto de vista administrativo, tenían las siguientes encomiendas:

> Llevar un libro de folio para registrar, de acuerdo a un plano, las calles comprendidas en su cuartel; llevar un registro de los comercios, mesones, casas de obradores, levantar un padrón de todos los vecinos y sus familias, eclesiásticos y seculares; anotar en un libro los fallecimientos ocurridos, pedir a los administradores de mesones un informe de todos los huéspedes, especificando su procedencia y destino; obligar a los indios a vivir dentro de sus parcialidades; velar por la limpieza de calles y cañerías; vigilar que hubiera en su barrio médico, cirujano, barbero, partera, boticario y escuela y que las viudas y huérfanos se recogieran con personas honestas o donde pudieran estos último aprender oficio. Como funciones de policía debían hacer rondas, impedir músicas en las calles, la embriaguez, y los juegos. Debían vigilar las vinaterías, pulquerías, fondas, almuercerías, mesones y trucos. Debían cooperar con los tenientes de la Acordada persiguiendo a los vendedores de bebidas embriagantes y a los portadores de armas prohibidas. También debían

[14] Gómez del Campo Díaz Barreiro, Bernardo, *op., cit.,* nota 5, *p*. 4.

> perseguir los contrabandos, auxiliar a los alcaldes de otros cuarteles y a los interventores de tributos, tanto en aprehender a los renuentes como en protegerlos de los insultos de la plebe, para todo lo cual podían requerir a los jefes militares el auxilio de las tropas.[15]

El 21 de septiembre de 1808 y teniendo como antecedente la invasión a España por parte del Emperador Napoleón, se crea en la capital del Reino de la Nueva España (Ciudad de México), la Junta Extraordinaria de Seguridad y Buen Orden. Fecha de nacimiento de nuestra policía. La Junta a la que nos referimos fue conformada por peninsulares militares que andaban a caballo, con espada y tras los que se opongan al dominio francés. Luego de unos años cambia su denominación a Junta de Policía y Seguridad:

> Su función explicita era la de garantizar la seguridad de la ciudad contra cualquier intento insurgente desestabilizador mediante la vigilancia y detención de individuos sospechosos, especialmente a aquellos simpatizantes de los insurgentes que apoyaban el regreso al gobierno monárquico español de Fernando VII y luchaban por la independencia de España, respecto de Francia.[16]

1.2.3. El México Independiente

Al saberse libres los verdaderos mexicanos lucharon contra el despotismo y la explotación de que eran víctimas, combatiendo al régimen monárquico, e implantando una república democrática, en donde los nacionales destituirían a los españoles del poder. Hay insurrecciones, cuartelazos y golpes de Estado, para esta fecha todo el sistema ha cambiado, ahora son libres y el sistema debe cambiar y los mexicanos con él. [17]

---

[15] Yáñez Romero, José Arturo, *Policía Mexicana,* México, Plaza Valdés Editores, 1999, p. 75.

[16] Andrés Martínez, Gerónimo Miguel, *op., cit.,* nota 1, p. 2.

[17] Ramírez Ramírez, Efrén, *op., cit*., nota 4, p. 120.

No obstante lo anterior, hasta el 6 de febrero de 1822 el régimen policial era depositado en jueces auxiliares. El 7 de febrero de 1822, se organizó un grupo de policía preventiva en la ciudad de México, que más tarde se les denominó Policías de Seguridad. Posteriormente en 1824 se creó el Bando de Policía y Buen Gobierno para formalizar la operación de la policía preventiva.[18]

Es en el primer cuarto del siglo XIX, cuando a decir del autor José Arturo Yañes Romero, en Puebla se crea el primer cuerpo que lleva en el nombre el propósito de la modernización policial: Policía de Orden y Seguridad, estos elementos que guardan rastros de la policía liberal, "se imponen después de la revolución francesa como un derecho ciudadano y una necesidad gubernamental".[19]

En diciembre de 1828, se expidió un reglamento, que según el artículo 12, establecía:

> Para la conservación del orden, se nombrara el vigilante y cuatro vecinos de cada calle de la manzana, para que ronden y cuiden diariamente aquello, alternándose entre el día y la noche de manera que no falten en ella, y se fijará en las esquinas la lista de los individuos a quienes les corresponde la ronda de la semana, expresándose el día que a cada uno le toca para el conocimiento de los vecinos y que puedan en caso necesario, demandar el auxilio de aquéllos.[20]

Casi para llegar a la mitad del siglo XIX, la inseguridad prevalecía en todas las regiones, asaltantes ponían en constante peligro la vida de los ciudadanos, de tal suerte que se delegó al pueblo la facultad de la persecución, para ello se enlistaron los propios ciudadanos para ser vigías de las ciudades, pueblos, haciendas y caminos.[21] Es entonces que en México aparecen las Gendarmerías en 1869:

---

[18] Gómez del Campo Díaz Barreiro, *op., cit.,* nota 5, p. 4.
[19] Yáñez Romero, José Arturo, *op.,* cit., nota 15, p. 62.
[20] Andrés Martínez, Gerónimo Miguel, *op., cit.,* nota 1, p. 27.
[21] Gómez del Campo Díaz Barreiro, Bernardo, *op., cit.,* nota 5, p. 5.

> Cuerpos de policía que se integraron con grupos de infantería y caballería, organizados en líneas verticales de mando con un jefe con competencia en tres o más distritos políticos, a cargo de un Comandante, un Guía, un Agente y Gendarmes dirigidos por un jefe responsable en la adopción de medidas para procurar seguridad y orden dentro de la entidad, en la organización de la policía local y coordinación de los trabajos.[22]

Durante esta época aparece por primera vez un conjunto de requisitos para ingresar en estos cuerpos de policía, a saber: [23]

1. Tener buena conducta.
2. Ser mayor de 21 años
3. Tener aptitudes físicas y mentales
4. Conocer el manejo de armas y caballos
5. No tener antecedentes penales.

Como era de esperarse y debido a los serios problemas provocados por la autonomía de las gendarmerías, en 1880, los Estados empiezan a legislar en materia de policía, así surgen nuevos reglamentos y leyes, con organizaciones novedosas que no produjeron ningún resultado, teniendo entonces que crear cuerpos de policía rural, cuyo resultado fue exactamente el mismo que las gendarmerías ya que, desde entonces los intereses políticos de algunos prevalecían sobre el bienestar de la mayoría.

1.3.4. La Policía en el México Posrevolucionario

En 1912, había iniciado el movimiento revolucionario, cosas inciertas estaban por venir; empero, es justo en ese momento cuando se otorgan todas las funciones encomendadas a los diversos cuerpos de policía existentes a la Guardia Nacional, hasta que se realiza un nuevo reglamento que entra en vigor en 1928.[24] Durante

[22] *Idem.*
[23] Andrés Martínez, Gerónimo Miguel, *op., cit.,* nota 1, p. 28.
[24] *Ibidem,* p. 29.

esta época, misma que corresponde al periodo presidencial de Francisco I. Madero, se creó el primer centro Social y Educativo de la Policía del Distrito Federal.[25]

Después de la lucha armada originada por la Revolución mexicana, se dan los primeros esbozos del México moderno. Cabe señalar que es aquí donde la figura de la policía por primera vez tiene un fundamento constitucional, un fundamento que prevalece al día de hoy y en el que se faculta a la policía como órgano investigador, en virtud de que previamente solo se basaba en ordenanzas y reglamentos. Brevemente el autor Efrén Ramírez Ramírez lo explica así:

> Comenzaron a tomar forma y a definir su contorno en el congreso constituyente, que se instalaría formalmente en la ciudad de Querétaro el 21 de noviembre de 1916. Don Venustiano Carranza presentó el proyecto de reforma a la constitución de 1857; en su parte medular estructuraba la nueva misión del Ministerio Público, al colocarlo como el único precursor de los delitos y dejando a su cargo la búsqueda de elementos de convicción, a la policía judicial. Así el México moderno comenzó a tomar forma con la Constitución de 1917, estableciendo la figura de la policía como auxiliar del Ministerio Público, en la investigación y persecución de los delitos.[26]

Habrá mucho que hablar en los años siguientes a la creación de la Constitución de 1917 acerca de la Policía, no obstante, la importancia que recobrará durante el mandato del General Lázaro Cárdenas del Río es cuando en 1939 el Cuerpo de Investigaciones y Seguridad Pública pasa a denominarse Servicio Secreto, cuyo funcionamiento y organización se encontraban regulados en el Reglamento Orgánico de la Policía Preventiva.[27]

En este reglamento se precisa que el servicio secreto se divide en dos secciones: “La primera comprende al grupo de abogados y empleados auxiliares y la segunda al grupo de agentes. También menciona que el servicio secreto se

[25] Torres Bravo, Sergio Ibán, *op., cit.,* nota 6, p. 75.
[26] Ramírez Ramírez, Efrén, *op., cit*., nota 4, p. 121.
[27] *Idem.*

auxiliaría de la policía uniformada en sus funciones preventivas y que su jurisdicción sería el Distrito Federal".[28]

En 1947, es surgida la Dirección Federal de Seguridad, como unidad especial de prevención e investigación a amenazas contra la seguridad nacional, específicamente casos de subversión comunista, Producto de la Segunda Guerra Mundial y el inicio de la Guerra Fría, institución ampliamente involucrada en los casos de narcotráfico en la década de los años 70`s y desaparecida en la década de los años 80`s por el entonces Presidente Miguel de la Madrid.[29]

1.3. La Policía Moderna

Por lo menos durante la última década del siglo pasado, la situación límite de inseguridad sufrida por todos, derivó en un sentimiento de inconformidad social que a la fecha ha ido en aumento, la escasa o nula respuesta de los órganos de seguridad pública se debió principalmente a que las instituciones públicas encargadas de proporcionar la misma, fueron infiltradas por el crimen organizado y se corrompieron.[30]

1.3.1. La Policía como Institución de Seguridad Pública

Para comprender a la *policía* en su significado de Institución de Seguridad Pública, hemos de considerar que:

> El Estado, por medio de las instituciones de seguridad pública, tiene constitucionalmente el uso exclusivo de la fuerza para mantener el orden público, y dar cumplimiento a las leyes y reglamentos. Debido a que la Constitución prohíbe

[28] *Idem.*
[29] Gómez del Campo Díaz Barreiro, Bernardo, *op., cit.,* nota 5, p. 6.
[30] Andrés Martínez, Gerónimo Miguel, *op., cit.,* nota 1, p.34

que los habitantes de un país se hagan justicia por sí mismos, o que ejerzan violencia para hacer valer sus derechos.[31]

En efecto, la seguridad pública de los gobernados se encuentra a cargo del Estado, y con ello se asegurara el orden público, lo anterior es elemental para mantener la paz y armonía en la convivencia social y para lograr el éxito es necesario mantener a la institución de la policía en un lugar destacado. "La policía es entonces un órgano, una institución de control social, cuya función es constituirse en uno de los mecanismos de lograr la seguridad pública, a través de ser un instrumento para obtener el orden público."[32]

"En materia de control social, la policía es considerada como uno de los medios de control que ejerce el gobierno dirigida hacia los ciudadanos, a la par de la Ley Penal, Los Tribunales y los Centros de Readaptación Social."[33] "Una de las características primordiales del Estado moderno es el monopolio del ejercicio de la actividad policial para regular la convivencia ciudadana. Sólo el Estado puede establecer, de manera legítima, normas y medidas coercitivas para mantener el orden y la seguridad."[34]

La reforma a la Constitución Mexicana en el año de 2008, penalmente y en el tema de la seguridad pública y de la policía, se inserta en la concepción de un Estado de Derecho democrático que propugna porque las instituciones de seguridad pública actúen bajo los principios de legalidad, objetividad, eficiencia, profesionalismo, honradez y respecto a los derechos humanos reconocidos en esta Constitución.[35]

---

[31] Ramírez Ramírez, Efrén, *Los Derechos Humanos en la formación de la Policía Judicial, manual de capacitación,* Porrúa, México, 2009, p. 115.

[32] Orellana Wiarco, Octavio A., *op., cit.,* nota 2, p. 75.

[33] Andrés Martínez, Gerónimo Miguel, *op., cit.,* nota 1, p. 141.

[34] Suárez De Garay, María Eugenia, *Los Policías: una averiguación antropológica,* México, ITESO, 2006, p. 117.

[35] Orellana Wiarco, Octavio A., *op., cit.,* nota 2, p. 76.

En relación a los principios que debe cumplir la policía, además de los principios ya consagrados, deberá considerar los que se refiere al respeto a los derechos humanos reconocidos por la propia constitución, es decir, adopta el criterio garantista de los derechos fundamentales del individuo.[36] Nuestra Constitución obliga a la policía y a todas las autoridades del país a respetar los derechos individuales de manera absoluta.[37]

1.3.2. Las funciones de la Policía

Dentro de las múltiples funciones que pueden ser atribuidas a la policía, se encuentran en su mayoría las que recaen directamente en mantener el orden en la sociedad, tenemos así que de acuerdo con André Bossard, citado por María Eugenia Suárez de Garay la principal función es: "Garantizar la paz y la seguridad en una colectividad, así como la seguridad de los ciudadanos, imponiéndoles por la fuerza si fuese necesario, la observancia de las leyes".[38]

Ahora bien, por otra parte, obsérvese a la policía como un cuerpo, en el que cada uno de los miembros que lo conforman, tendrán a su cargo funciones específicas, en cuyo componente se demostrará la certeza de seguridad que se brinda a la ciudadanía. En acuerdo con el autor Efrén Ramírez Ramírez, tenemos que la Policía es el cuerpo creado para mantener el orden público y debe: "proteger a las personas y sus bienes; mantener la tranquilidad y el orden público; salvaguardar el ejercicio de las libertades públicas y actuar como auxiliar de la justicia".[39]

Por otra parte, algunos autores, indican que las funciones de los servicios policiales son múltiples y variadas, pero en muchos casos puede situarse entre cuatro categorías y para el caso concreto se pueden analizar de la siguiente

---

[36] *Idem.*
[37] Ramírez Ramírez, Efrén, *op., cit.,* nota 31, p. 118.
[38] Suárez de Garay, María Eugenia, *op., cit.,* nota 34, p. 117.
[39] Ramírez Ramírez, Efrén, *op., cit.,* nota 31, p. 118.

manera: prevenir el delito, reprimir el delito, mantener el orden y auxilio y asistencia social.

La ciencia de la policía consiste en regular todo lo que se relaciona con el estado presente de la sociedad, consolidarla, mejorarla, para que todo concurra a la felicidad de los miembros que la componen.[40] Sobre el papel de la policía en la actualidad, Mazzitelli expresa:

> Para dar respuesta a estas demandas, las policías de los estados modernos deben contar con recursos humanos adecuados, hombres y mujeres altamente capacitados y entrenados que tengan a su disposición herramientas de investigación y de información acordes con los desarrollos modernos de las era moderna. Deben contar adicionalmente, con un marco legal y reglamentario que les permita operar de manera eficiente en el contexto de apego a los límites que impone el estado de derecho.[41]

1.3.3. La Policía Federal Preventiva

La Policía Federal Preventiva (PFP), es la Institución Policial que fue creada el 13 de diciembre de 1998, dentro de la Secretaría de Gobernación, bajo el mandato del Presidente Ernesto Zedillo Ponce de León, su creación como apoyo operativo en la lucha contra la delincuencia organizada. En el año 2000 se adscribió orgánicamente a la Secretaría de Seguridad Pública federal, cuyas finalidades serán básicamente la prevención de delitos en materia del fuero federal, aunque su labor fue reconocida en todo el país, ya que su eficiencia era notoria.

Se dice que para la creación de la PFP, se fusionaron la Policía Federal de Caminos, Policía Fiscal y además se le integró personal proveniente de la Armada de México; empero, manifiesta Marcelo Bergman, que la Policía Federal Preventiva

---

[40] Yáñez Romero, José Arturo, *op.,* cit., nota 15, p. 38.

[41] Rabasa Gamboa, Emilio, *et al, El marco jurídico de la Seguridad Pública en México,* México, Editorial Porrúa, 2012, p. 58.

se integró además de policías que originalmente pertenecían a las fuerzas de seguridad preventiva, elementos de la Federal de Caminos y de la Policía Fiscal, por la policía migratoria y algunos del CISEN (Centro de Investigación y Seguridad Nacional).[42]

Su ámbito de competencia sería entonces todo el territorio nacional, exclusivamente lo que se refiere a la materia federal, y con estricta observancia de las esferas y funciones que constitucional y legalmente corresponden a las entidades federativas y a los municipios. Para lo anterior podría y debía suscribir convenios de colaboración con las autoridades respectivas.

La PFP, se estructuraba orgánicamente en cuatro Coordinaciones Generales, las tres primeras se encargaban de realizar funciones operativas, todas aquellas situaciones que se encontraran directamente relacionadas con el cumplimiento de los propósitos para los que fue creada esta institución y la última se encargaba de la profesionalización de los elementos que integraban la corporación policial, así tenemos a:

Coordinación General de Inteligencia para la Prevención
Coordinación General de Seguridad Regional
Coordinación General de las Fuerzas Federales de Apoyo
Coordinación General del Instituto Profesional.

La Función de la PFP, surge como un elemento central de la estrategia de Estado para combatir al narcotráfico, garantizar, mantener y restablecer el orden público, con una esfera de competencia claramente delimitada a las funciones “de salvaguardar la integridad y derechos de las personas, prevenir la comisión de delitos, así como preservar las libertades, el orden y la paz públicos”.[43]

[42] Bergman, Marcelo, *Seguridad Pública y Estado en México, análisis de algunas iniciativas,* 2ª ed., México, Editorial Fontamara, 2011, p. 71
[43] Andrés Martínez, Gerónimo Miguel, *op., cit.,* nota 1, p. 810.

1.3.4. La Agencia Federal de Investigación

La Agencia Federal de Investigación (AFI) fue creada por un Decreto del Ejecutivo, publicado el 1 de noviembre de 2001 en el Diario Oficial de la Federación, con la función de ser un auxiliar del Ministerio Público de la Federación en la procuración de justicia y el combate de los delitos de orden federal.[44]

La AFI, tiene su origen en la Dirección General de Planeación y Operación de la Policía Judicial Federal, la que a su vez tuvo un prolongado desarrollo constitutivo que parte desde la época colonial, y cuyos objetivos y antecedentes han evolucionado paralelamente al devenir histórico del Ministerio Público y del procedimiento penal.[45]

"La AFI surge como una policía profesionalizada, con facultades, recursos y capacidades para realizar actividades de investigación e inteligencia."[46] La AFI se integraba jerárquicamente, por:

Dirección General de Planeación Policial
Dirección General de Investigación Policial
Dirección General de Análisis Táctico
Dirección General de Despliegue Regional Policial;
Dirección General de Operaciones Especiales

1.4. La Policía Federal

Con la reforma constitucional en materia de justicia penal y seguridad pública, en 2008, se hizo necesario realizar modificaciones a otras legislaciones tendientes a consolidar la actuación y unificación de las corporaciones de policías. Desaparece

[44] Diario Oficial de la Federación, en *http://dof.gob.mx/nota_detalle.php?codigo=757798&fecha=01/11/2001*
[45] Bergman, Marcelo, *op., cit.,* nota 42, p. 79
[46] *Idem.*

lo que conocíamos como Agencia Federal de Investigación (AFI), que era la facultada para investigar conductas delictivas de tal orden, para cambiar de denominación y llamarse Policía Federal Ministerial con las facultades de investigación que correspondían a la AFI*,* pero con cambios sustanciales que le permiten una investigación más definida, acorde a un sistema penal acusatorio.[47]

Asimismo, se abroga la llamada *Ley de la Policía Federal Preventiva* para ahora denominarse *Ley de la Policía Federal,* por lo cual las facultades de la policía quedan unificadas en la institución de la policía como tal, contempladas en el artículo 8º de la Ley de la Policía Federal.[48] La Ley de la Policía Federal es de orden público y de aplicación en todo el territorio nacional y reglamentaria del artículo 21 Constitucional en materia federal; su objetivo es la organización y funcionamiento de la Policía Federal que es un órgano administrativo desconcentrado dependiente de la Comisión Nacional de Seguridad.[49]

El artículo 2 de la Ley de la Policía Federal, publicada en el Diario Oficial de la Federación el 1 de junio de 2009, indica que la Policía Federal, es un órgano administrativo desconcentrado de la Secretaría de Seguridad Pública, (hoy la Comisión Nacional) y sus objetivos serán los siguientes:

---

[47] Maldonado Sánchez, Isabel, *La Policía en el Sistema Penal Acusatorio, investigación científica del delito y custodia de la evidencia,* 2ª ed., México, Palacio del Derecho Editores, 2010, p. 81.

[48] *Idem.*

[49] Se crea la Comisión Nacional de Seguridad tomando en cuenta que mediante Decreto publicado el 2 de enero de 2013 en el Diario Oficial de la Federación, en cuyo Artículo 27 fracción XII, se indica que será responsabilidad de la Secretaría de Gobernación "Formular y ejecutar las políticas, programas y acciones tendientes a garantizar la seguridad pública de la Nación y de sus habitantes"**.** Asimismo, estará dentro de la esfera de esta dependencia proponer al Ejecutivo Federal la política criminal y las medidas que garanticen la congruencia de ésta entre las dependencias de la Administración Pública Federal. Coadyuvará a la prevención del delito, ejercer el mando de la fuerza pública para proteger a la población ante todo tipo de amenazas y riesgos, con plena sujeción a los derechos humanos y libertades fundamentales; salvaguardar la integridad y los derechos personales, así como preservar las libertades, el orden y la paz públicos. La fracción XIII bis establece que deberá proponer acciones para asegurar la coordinación entre la Federación, el Distrito Federal, los Estados y los Municipios en el ámbito del Sistema Nacional de Seguridad Pública.

I. Salvaguardar la vida, la integridad, la seguridad y los derechos de las personas, así como preservar las libertades, el orden y la paz públicos;

II. Aplicar y operar la política de seguridad pública en materia de prevención y combate de delitos;

III. Prevenir la comisión de los delitos, y

IV. Investigar la comisión de delitos bajo la conducción y mando del Ministerio Público de la Federación, en términos de las disposiciones aplicables.

El viernes 6 de julio de 2012, se publicó en el *Diario Oficial de la Federación* el manual de organización general del órgano administrativo desconcentrado Policía Federal, cuyo índice se describe a continuación:

I. Antecedentes
II. Marco Jurídico-Administrativo
III. Atribuciones
IV. Misión y Visión
V. Estructura Orgánica (Anexo 1)
VI. Organigrama
VII. Objetivos y funciones por área
VIII Glosario

Citado por Gerónimo Miguel Andrés Martínez, el autor Arturo Aragón sostiene que esta función está mal planteada, porque la AFI tenía la función de investigación y la PFP de prevención, "no va a funcionar, y aun cuando se llamará PFP o Policía Federal en su conjunto, de todos modos tendrá que tener las dos áreas." [50]

1.4.1. La Policía Cibernética

En México, existe desde el año 2000 una policía cibernética que originalmente se encontraba adscrita a la Coordinación General de inteligencia para

[50] Andrés Martínez, Gerónimo Miguel, *op., cit.,* nota 1, p. 823.

la Prevención de, la entonces Secretaria de Seguridad Pública, hoy denominada *Comisión Nacional de Seguridad Pública*, cuyas actividades principales consisten en: "Patrullar Internet para rastrear conductas ilícitas, portales, comunidades y *chat romos* en los que se promueven la pornografía y el turismo sexual infantil en territorio nacional".[51] Cabe aclarar que dicha creación se da sin ningún marco legal que la regule.

Del centro y sur de América, México fue el primer país en crear un cuerpo policial de este tipo, el que hoy pende de la estructura orgánica de la Policía Federal, por lo que la ubicamos en el organigrama dentro de la Dirección General de Prevención de Delitos Cibernéticos, adscrita a la Coordinación para la Prevención de Delitos Electrónicos de la División Científica de la Policía Federal. (Anexo 2)

A propósito de la policía cibernética rescátese el trabajo que realiza esta policía, como lo señala Gerónimo Miguel Andrés Martínez, en la manera de operar:

> La Policía Cibernética opera a través de patrullajes *antihacker* por el ciberespacio, a través de computadoras, con lo que han comprobado el alarmante crecimiento de organizaciones de pedófilos que transmiten pornografía infantil y promueven la corrupción de menores vía Internet. Dicho "ciberpatrullaje" sirve también para atrapar a los delincuentes que cometen fraudes, intrusiones y organizan sus actividades delictivas en la red, sin que necesariamente se dediquen a la pornografía infantil. También se han detectado bandas internacionales de prostitución, que utilizan sistemas informáticos como medio de promoción y sobre todo de reclutamiento.[52]

Como se ha mencionado, dentro de las finalidades para las que fue creada la policía cibernética, la entonces Policía Federal Preventiva, buscaba identificar y desarticular bandas dedicadas al robo, lenocinio, tráfico y corrupción de menores,

---

[51] Velasco San Martín, Cristos, *La jurisdicción y competencia sobre delitos cometidos a través de sistemas de cómputo e internet,* México, Tiran lo Blanch, 2012, p. 299.

[52] Andrés Martínez, Gerónimo Miguel, *op., cit.,* nota 1, pp. 824-825.

así como la elaboración, distribución y promoción de pornografía infantil, por cualquier medio, y con el auge que cobró la utilización de los medios tecnológicos en las últimas décadas, no hay más que hurgar en la red más grande del mundo, Internet.

Gracias a la colaboración con los *ciberpolicías* en otros países se ha logrado que con cada detención hecha en algún lugar del mundo ubiquen las conexiones que tienen los delincuentes en México e incluso con la colaboración de organismos no gubernamentales, quienes por su cuenta realizan *ciberpatrullajes* en la red, que han localizado sectas satánicas que utilizan menores y animales en sus sacrificios.[53]

La policía cibernética intercambia datos con organizaciones internacionales como el *National Center For Missing and Exploited Children*, (Centro Nacional para niños perdidos y explotados) de Estados Unidos, que ha ayudado identificar grupos de pedófilos en el Estado de California.

[53] *Ibidem* p. 824.

CAPÍTULO 2. DE LOS DELITOS CIBERNÉTICOS, INFORMÁTICOS O CIBERDELITOS

2.1. Generalidades sobre Internet y Ciberespacio

2.1.1. Internet

A medida que el tiempo avanza y la tecnología evoluciona, surge la necesidad de crear conceptos para darle un significado a los nuevos conocimientos, el Internet es una herramienta difícil de ser unificada conceptualmente, debido a que se han generado un gran número de definiciones. En términos generales se puede definir como:

> Un sistema global descentralizado de redes de cómputo interconectadas entre sí, con base en los estándares o protocolos conocidos como Protocolo de Transmisión de Control (TCP) y el Protocolo Internet (IP) que se utilizan para transmitir e intercambiar paquetes de datos. Internet se le conoce como la red de redes y actualmente consiste en millones de redes de cómputo públicas, privadas, académicas corporativas y gubernamentales que están vinculadas o conectadas entre sí, a través de fibra óptica, conexiones inalámbricas y otras tecnologías.[54]

Por otro lado, el autor Enrique Nava Garcés, retoma el concepto del avance de la vigésima tercera edición del diccionario de la Real Academia Española, que define como: “Una red informática mundial, descentralizada, formada por la conexión directa entre computadoras u ordenadores, mediante un protocolo especial de comunicación”.[55]

El mismo autor indica que también puede definirse como: “Un conjunto de elementos tecnológicos que permite enlazar masivamente redes de diferentes tipos

[54] Velasco San Martín, Cristos, *op., cit.*, nota 51, p. 33.

[55] Nava Garcés, Alberto Enrique, *La prueba electrónica en materia penal,* México, Porrúa, 2011, p. 9.

para que los datos puedan ser transportados de una a otra red".[56] Definición llana y que para efectos de la presente investigación es la más simple de ser asimilada.

Habrán muchos términos y conceptos conocidos y dominados por la mayor parte de la gente usuaria de la red en el mundo, sin embargo, hay otros miles que aunque son conceptos que dan vida virtual a una serie de acciones que los usuarios de Internet ejecutan día a día, aun son desconocidos para entender más a fondo podemos observar los protocolos y los conceptos básicos que son presentados en el Anexo 3 de la presente investigación.

2.1.2. Ciberespacio

"El término ciberespacio fue acuñado por el escritor William Gibson (en 1984) y es una metáfora para describir el terreno no físico creado por sistemas de computadora."[57] "Tras la publicación de una obra de ciencia ficción de 1982, denominada *"Burning Chrome"* y popularizada a través de otra de sus obras en 1984 *"Neuromancer."* [58]

Por su parte, Lawrence Lessing en su libro *Code and other Laws of Cyberespace*, señala:

> El ciberespacio no es un lugar. Es muchos lugares distintos. La forma de estos muchos lugares no es idéntica. Está conformado de diferentes maneras, esto resulta fundamental. Estas diferencias resultan en parte por la gente que puebla los diversos lugares que lo conforman, pero la situación demográfica no puede por sí sola explicar estas variantes. Hay en el ciberespacio la conjunción de más elementos variables.[59]

[56] *Idem.*
[57] *Ibidem* p. 10.
[58] Velasco San Martín, Cristos, *op., cit.*, nota 51, p. 34.
[59] Nava Garcés, Alberto Enrique, *op., cit.*, nota 55, p. 10.

En un sentido amplio, el ciberespacio actualmente forma parte del lenguaje técnico, y comúnmente se utiliza para referirse a los contenidos y actividades que acontecen en Internet, el concepto por sí mismo de inmediato hace que se cree un vínculo y asociación con sistemas de cómputo, tecnologías de la información, y las actividades que tienen lugar a través de Internet, sin tener en cuenta la ubicación física y geográfica de los servidores, operadores y actores.[60]

En el contexto de la regulación del espacio, es decir, desde una perspectiva jurídica, esencialmente Alfredo Calderón Martínez, admite que el ciberespacio: "Es el lugar donde algunos delitos informáticos pueden ser cometidos, prevenidos y detectados".[61]

Para algunos autores el ciberespacio no debe ser regulado por las leyes en vigencia, tal es caso de John Perry Barlow, quien se manifiesta en contra de la aplicación y ejecución de la legislación americana a actividades que acontezcan en el ciberespacio, argumentando que el ciberespacio es propiamente un espacio independiente que se encuentra fuera de los límites geográficos de la soberanía estatal y por tanto, fuera de control y la regulación gubernamental.[62]

Es menester precisar que Internet y ciberespacio se encuentran profundamente vinculados, debido a que Internet es la herramienta con la que se puede tener acceso al ciberespacio:

> Muchas actividades y conductas que acontecen en el ciberespacio tienen una repercusión en los sujetos y entidades que forman parte del mundo real y que se encuentran regidos por una normatividad creada y controlada por el Estado a través de su propio sistema jurídico.[63]

---

[60] Velasco San Martín, Cristos, *op., cit.*, nota 51, pp. 35-36.
[61] Nava Garcés, Alberto Enrique, *El Derecho en la era digital*, México, Porrúa, 2013, p. 4.
[62] Velasco San Martín, Cristos, *op., cit.*, nota 51, p. 36.
[63] *Idem.*

2.2. Delitos cibernéticos, informáticos o ciberdelitos

2.2.1. Derecho Binario o Informático

El Derecho como una ciencia, indudablemente, requiere estar en constante transformación, adaptándose a los cambios que de forma consuetudinaria se generan en el entorno social y jurídico, lo cual a su vez propicia que se tengan que perfeccionar las áreas del conocimiento y es por ello, que como resultado de transformaciones, que se han generado con el estallamiento de la era digital, surge el denominado por el autor Carlos Antonio Vázquez Azuara, Derecho Binario[64], como una nueva rama del derecho, que tiende a enfocar su estudio a la regulación jurídica del individuo relacionada con las nuevas tecnologías y el Internet.[65]

> El Derecho Binario, es la rama del derecho que se encarga del estudio de las normas que regulan la relación entre los individuos basada en su realidad virtual y de ellos con dicha realidad, así como el estudio de las normas que regulan la conducta de los individuos basada en las nuevas tecnologías e Internet.[66]

Por otra parte, siguiendo en el mismo orden de ideas, tenemos una denominación distinta para aquellas normas que pueden regular la era de la tecnología, aceptando un concepto, que en esencia tiene que ver con nuestro concepto anterior y así citamos al profesor Mario Vasconcelos, quien señala que: "La expresión *Informática Jurídica* también se le denomina *Derecho Informático* y

---

[64] *El Derecho Binario*, se denomina como tal, puesto que, el único enlace que existe entre el hombre y la era digital, es un código denominado código binario, es decir, aquel constituido por unos y ceros, de ahí que se denomine binario. Pues bien, el Código Binario, permite a los medios digitales comprender las instrucciones dadas por el ser humano, es decir, es el lenguaje específico que se necesita para que un ordenador comprenda las instrucciones dadas por la parte humana. Cuando vemos en nuestro monitor un documento de un procesador de textos común y se advierte una hoja, con regla y márgenes, lo que estamos viendo evidentemente es para comprensión de los ojos del usuario, pero la realidad, es que lo que vemos en un trasfondo es una secuencia de unos y ceros. Por tanto, al ser el Código Binario, el único medio que permite la manifestación de la era digital tal y como la conocemos, es que resulta correcto denominar a la nueva Rama del Derecho de la que se viene hablando, como Derecho Binario.

[65] Vázquez Azuara, Carlos Antonio, *Combate a la Delincuencia Cibernética,* México, Editorial Universidad de Xalapa, 2012, p. 24.

[66] *Ibidem,* p. 43.

se refiere a la reglamentación, racional y científica, de la comunicación". [67] Comprende, por ende lo vinculado con la computación.

Es preciso mencionar que el *Derecho Informático*, también tiene su origen como nueva rama del Derecho, gracias a que es necesario regular los bienes informacionales, consecuentemente es indispensable su tratamiento jurídico en virtud de su innegable carácter económico, siendo necesaria la protección de datos personales, la protección de programas, solución a los problemas provocados por la llamada piratería, los delitos informáticos en sentido amplio. Así como la comisión de verdaderos actos ilícitos en los que se tenga en la computadora un instrumento o fin.[68]

Así entonces para efectos de esta investigación, al analizar las propuestas para los términos empleados, adoptaremos la que de manera tradicional podría definirse en *Derecho Informático*: conjunto de normas jurídicas encargadas de regular las conductas suscitadas en el ciberespacio. No es óbice mencionar que previo a este concepto se ha mostrado un panorama general de lo que es el ciberespacio.

2.2.2. Definición de Delito

Pugnamos por partir de la doctrina para determinar que es un delito y así poder construir la definición de *delito cibernético, informático o ciberdelito*, tenemos así que el Profesor Günter Jakobs, no expone en ningún momento un concepto determinado de delito y de sus distintos elementos; sin embargo, una aproximación a su pensamiento hace posible entender al delito como:

---

[67] Nava Garcés, Alberto Enrique, *Análisis de los delitos cibernéticos,* México, Porrúa, 2005, p.17

[68] Cassou Ruíz, Esteban, *Delitos informáticos en México*, Revista del Instituto de la Judicatura Federal, Núm. 28. p. 225, disponible en: http://www.ijf.cjf.gob.mx/publicaciones/revista/28/Delitos_inform%C3%A1ticos.pdf

> La expresión simbólica de una falta de fidelidad hacia el derecho, una amenaza para la integridad y estabilidad social, comportamiento que defrauda las expectativas que genera un estatus social, defraudación de una expectativa, rebelión contra la norma o quebrantamiento de la vigencia normativa.[69]

De tal suerte que el criterio legalista desplaza la definición del campo del jurista hacia el del titular del órgano legislativo. Por lo que para efectos de esta investigación se pretende una construcción desde un corto número de palabras, hasta llegar a la definición de delito en su concepción jurídica, observemos como fue su evolución hasta adquirir el valor con el que hoy día se conoce, esto es que para Albert Brener el delito es una acción; para Rudolph Ihiering una acción antijurídica; ya un poco más valorado para Fran Von Liszt el delito es una conducta antijurídica y culpable;[70] Ernesto Beling señaló en el año de 1906, la acción típica, antijurídica, culpable sometida a una adecuada sanción penal y que llena las condiciones objetivas de punibilidad;[71] finalmente Jiménez de Asúa, citado por Castellanos Tena, textualmente define: "*Delito es el acto típicamente antijurídico culpable, sometido a veces a condiciones objetivas de penalidad, imputable a un hombre y sometido a una sanción penal*".[72]

Al realizar el análisis y expuesto lo anterior, se observa que la construcción jurídica del delito es la *"acción o conducta típica, antijurídica, culpable y punible".*[73] Se concluye que la definición que comprende de manera amplia y general los elementos necesarios para poder llamar a una conducta socialmente reprobable será la que se ha expuesto en las líneas anteriores.

---

[69] Jiménez Martínez, Javier, *La teoría del delito, aproximación al estado de la discusión,* México, Porrúa, 2010, p. 224.

[70] Díaz Aranda, Enrique, *Derecho Penal Parte General,* 3° ed., México, Porrúa, 2012, p. 115.

[71] Arilla Bas, Fernando, *Derecho Penal,* 2ª ed., México, Porrúa, 2011, p.191.

[72] Castellanos Tena, Fernando, *Lineamientos elementales de Derecho Penal*, 35ª ed., México, Porrúa, 2012, p. 115.

[73] Pavón Vasconcelos, Francisco, *La Causalidad en el delito,* 5ta ed., México, Porrúa, 2004, p.112.

2.2.3. Definición de delitos cibernéticos, informáticos o ciberdelitos

Aun cuando en el subcapítulo anterior se ha presentado una definición de que es el delito, es complicado determinar cuál es la denominación correcta para las acciones de esta naturaleza, en virtud de que, tal como la manifiesta Cristos Velasco San Martín: "En algunos países se utiliza la expresión *delitos informáticos*, en otros se habla de *ciberdelitos* o *cibercrimen* o simple y llanamente delitos cometidos a través de sistemas de cómputo e Internet *(computer crime)*".[74] Y para muchos también son nombrados *delitos cibernéticos*.

"Desafortunadamente, no hay una definición unánime, todas las existentes se hicieron tomando en cuenta diferentes criterios, dependiendo de las perspectivas y experiencias tanto de quienes investigan este delito, como de quienes han sido víctimas del mismo."[75] Dicho lo cual, optaremos por incluir las varias definiciones a fin de considerar la más conveniente.

Ahora bien, obsérvese a continuación, algunas definiciones sugeridas por juristas, principalmente de habla hispana:

Tenemos al autor mexicano, Julio Téllez Valdés, quien aduce que se trata de *delitos cibernéticos* mismos que son: "actitudes ilícitas en que tienen a las computadoras como instrumento o fin", (concepto atípico) o las "conductas típicas, antijurídicas y culpables que tienen a las computadoras como instrumento o fin (concepto típico).[76]

Por su parte el autor Argentino Gabriel Andrés Campoli, indica también como *delitos cibernéticos*: "Aquéllos en los cuales el sujeto activo lesiona un bien jurídico

[74] Velasco San Martín, Cristos, *op., cit.*, nota 51, p. 50.
[75] Nava Garcés, Alberto Enrique, *op., cit.*, nota 55, p. 2.
[76] Téllez Valdés, Julio, *Derecho Informático,* 4ta ed., México, Editorial Mc Graw Hill, 2008, pp. 187-188.

que puede o no estar protegido por la legislación vigente y que puede ser de diverso tipo por medio de la utilización indebida de medios cibernéticos".[77]

Cabe hacer mención que para este autor existe otra categoría de delitos, los que se han nombrado *electrónicos o cibernéticos electrónicos*, y que manifiesta son una especie del género delitos cibernéticos, en los cuales el autor produce un daño o intromisión no autorizada en equipos electrónicos ajenos y que a la fecha por regla general no se encuentran legislados, pero que poseen como bien jurídico tutelado en forma específica la integridad de los equipos electrónicos y la intimidad de sus propietarios. [78]

Porras Quintela expresa: "Hay personas que consideran que los delitos informáticos, como tales, no existen. Argumentan que tan sólo son delitos normales que en lo único que se pueden diferenciar, de otro delito cualquiera, es en las herramientas empleadas o en los objetos sobre los que se producen."[79]

Para David Wall, quien a decir de Calderón Martínez, está de acuerdo con la idea de que no es posible construir una definición aceptada globalmente, entiende los *delitos informáticos* como: "Las actividades criminales o nocivas que involucran la adquisición o manipulación de la información para obtener un lucro."[80]

María Cinta Castillo y Miguel Ramallo aducen: "*Delito informático* es toda acción dolosa que provoca un perjuicio a personas o entidades en cuya comisión intervienen dispositivos habitualmente utilizados en las actividades informáticas."[81]

---

[77] Cassou Ruíz, Esteban, *op., cit.*, nota 68, p. 221.
[78] *Idem.*
[79] Nava Garcés, Alberto Enrique, *op., cit.*, nota 55, p. 21
[80] Nava Garcés, Alberto Enrique. *op., cit.,* nota 61, p. 3.
[81] Ponencia preparada en conjunto con los profesores argentinos Guillermo Beltramone y Ezequiel Zabale, y presentada en el X Congreso Latinoamericano y II Iberoamericano de Derecho Penal y Criminología, celebrado en la Universidad de Chile en agosto de 1998.

Los autores chilenos Marcelo Huerta y Claudio Líbano definen los *delitos informáticos* como:

> Todas aquellas acciones u omisiones típicas, antijurídicas y dolosas, trátese de hechos aislados o de una serie de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de la información y destinadas a producir un perjuicio en la víctima a través de atentados a la sana técnica informática, lo cual generalmente, producirá de manera colateral lesiones a distintos valores jurídicos, reportándose, muchas veces, un beneficio ilícito en el agente, sea o no de carácter patrimonial, actúe con o sin ánimo de lucro.[82]

El español, Davara Rodríguez define al *delito informático* como:

> La realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea *hardware* o *software*. Además, agrega que el delito informático es aquel que se comete utilizando bienes o servicios informáticos.[83]

Por su parte Nidia Callegari, define al *delito informático* como: "Aquel que se da con la ayuda de la informática o de técnicas anexas".[84] De la definición anterior podemos observar cómo es que, a decir de Nava García, el delito se vale de la tecnología para ser ejecutado, de tal suerte que sin la técnica y ciencia que implica la tecnología, no sería posible su comisión.

Ahora bien, baja esa tesitura entonces veamos que para María de la Luz Lima considera:

> El delito electrónico en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como

[82] *http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf*
[83] Velasco San Martín, Cristos, *op., cit.*, nota 51, p. 52.
[84] Nava Garcés, Alberto Enrique, *op., cit.,* nota 67, p. 20.

> método, medio o fin y que en un sentido estricto: El delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan ya sea como método, medio o fin.[85]

Nos explica Nava Garcés que la autora deja entonces al delito informático como una subespecie del delito electrónico, haciendo una fusión de la tecnología y de la electrónica como conceptos. Y sin embargo se puede observar que el delito informático tiene una gama más amplia para su existencia ya que se establece como método, es decir, entendiendo esta acepción como un modo de obrar o hacer, que en sentido laxo nos explica la actividad ilícita a través de un obrar con el uso de las computadoras u ordenadores. Esta idea nos remite a la segunda acepción que es usar la computadora como un medio, lo que consideramos, reitera la primera concepción. Y aparece una tercera opción, el uso de las computadoras como un fin de la conducta ilícita.[86]

Rodolfo Herrera Bravo en relación al tema, aduce que de la relación entre el delito e informática surgen dos tipos de ilícitos, los delitos computacionales y los delitos informáticos tenemos así que:

> Cuando los delincuentes de delitos tradicionales comienzan a utilizar como un medio especifico de comisión a las tecnologías de la información, se produce una informatización de los tipos tradiciones, naciendo el delito computacional, que en realidad se trataría solo de ilícitos convencionales que ya están regulados en el Código Penal. Sin embargo también se crean conductas nuevas, no contempladas en los ordenamientos penales por su especial naturaleza, lo que hace necesario crear los llamados *delitos informáticos.*[87]

Muchos países, incluidos los de habla hispana como son México y España, rebasados por lo que el uso de la tecnología ha implicado en el ámbito legal, han

---

[85] Nava Garcés, Alberto Enrique, *op., cit.,* nota 55, p. 35.
[86] *Idem.*
[87] Velasco San Martín, Cristos, *op., cit.*, nota 51, p.53.

tratado de encuadrar estas novedosas acciones en figuras típicas de carácter tradicional tales como, robo, fraude, falsificación, daños, estafa, sabotaje, etcétera. [88] No obstante lo anterior, es menester dar un nombre a estas conductas, y que si bien no pueden se unánime, cuando menos permitan una identidad, pues como se observa, aun compartiendo mismo idioma es una gama interminable de opiniones acerca de cómo deben ser llamados. Por tanto, para finalizar tenemos entonces que los *delitos cibernéticos, informáticos y ciberdelitos,* tienen como denominador común el uso de la *computadora e Internet y todo lo que de ellos deriva,* para realizar *actividades criminales.*

2.2.4. Definiciones de Organismos Internacionales para los delitos cibernéticos, informáticos o ciberdelitos.

La Convención Europea sobre el Delito Informático es el principal cuerpo normativo internacional que tipifica los delitos, relativos a este capítulo, sin embargo no proporciona una definición al respecto.

El grupo de expertos de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) creando su propia definición proponen que: "*El delito informático*, es cualquier conducta ilegal, no ética o no autorizada que involucra el procesamiento automático de datos y/o la transmisión de datos".[89]

En la recomendación del Consejo de Europa No. R (95) 13 aprobada por el Comité Europeo sobre Problemas de Delincuencia (CDPC) concerniente a problemas sobre derechos procesal penal en su 44ª sesión plenaria de Mayo 29 al 2 de junio de 1995, se utiliza el término *delitos relacionados con las Tecnologías de Información*, y los describe de la siguiente forma:

[88] Nava Garcés, Alberto Enrique, *op., cit.,* nota 55, p. 37.

[89] En 1986 dicha para la Cooperación y el Desarrollo Económicos emitió una recomendación sobre crimen relacionado con sistemas de cómputo en donde se contempló dicha definición.

> Contemplan cualquier conducta penal en una investigación en la cual las autoridades investigadoras tienen que obtener acceso a información que es procesada o transmitida en sistemas de cómputo o sistemas electrónicos de procesamiento de datos.[90]

La Unión Internacional de Telecomunicaciones (UIT) define al *delito informático* (*computer relater crime*) como: "Aquel cuyo objeto o medio de realizarlo es un sistema informático, está relacionado con las tecnologías digitales y se integra en los propios de la delincuencia de cuello blanco".[91] No obstante, también dicho organismo alude que el *ciberdelito* es una forma de *delito informático* que recurre a las tecnologías de Internet para su comisión, refiriéndose entonces a todos los delitos cometidos en el ciberespacio.

Por tanto es necesario, en el presente trabajo, adherirnos a una de las propuestas presentadas por los Organismos Internacionales y con la que se consigue una armonía es aquella que señala que: El *delito informático*, es cualquier conducta ilegal, no ética o no autorizada que involucra el procesamiento automático de datos y/o la transmisión de datos, a la que podríamos agregar que se refiere a todas los delitos cometidos en el ciberespacio, teniendo así una construcción que convenza en términos generales.

2.2.5. Clasificación de los delitos cibernéticos, informáticos o ciberdelitos

Una vez establecida la concepción de los delitos de esta naturaleza, aunque no de manera unánime, observaremos las clasificaciones que al respecto han aportado los tratadistas del tema, mismas se centran en la actividad del sujeto y no en el ámbito espacial en que ocurre dicha conducta.

---

[90] *Véase: http://www.cybercrimelaw.net/documents/cybercrime_history.pdf*

[91] Unión Internacional de Telecomunicaciones (*ITU Toolkit for Cybercrime Legislation por sus siglas en inglés*)

En primer lugar, obsérvese a Julio Téllez Valdés quien clasifica a los *delitos informáticos* con base en dos criterios, el primero como instrumento o medio, teniendo que *las conductas criminógenas que se valen de las computadoras como método, medio, o símbolo en la comisión del ilícito,* y el segundo criterio por su fin u objetivo, en esta categoría se enmarcan *las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física*.[92]

María de la Luz Lima clasifica lo que ella llama, como se ha visto anteriormente, *delitos electrónicos,* en tres categorías, y al no haber una diferencia sustancial entre método y medio, se advierte que su clasificación se refiere a medios y fines, a saber: [93]

> Los que utilizan la tecnología electrónica como método, esto es, conductas criminógenas en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito;
> Los que utilizan la tecnología electrónica como medio, donde podemos encuadrar las conductas criminógenas en donde para realizar un delito utilizan una computadora como medio o símbolo; y
> Los que utilizan la tecnología electrónica como fin. Aquí se podrán hallar las conductas criminógenas dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla.

Ahora bien, Correa retoma de manera descriptiva el trabajo de Sieber y refiere una clasificación *delitos informáticos* no genérica, más bien, determina las características de delitos en particular, ya que se refiere a conductas perfectamente definidas. Así tenemos las siguientes categorías: [94]

> Fraude por manipulaciones de un computador contra un sistema de procesamiento de datos;

---

[92] Nava Garcés, Alberto Enrique, *op., cit.,* nota 67, p. 26.
[93] *Idem.*
[94] *Ibidem,* p. 27.

Espionaje informático y robo de software;
Sabotaje informático;
Robo de servicios;
Acceso no autorizado a sistemas de procesamiento de datos, y
Ofensas tradicionales en los negocios asistidos por computador.

Por otra parte Palazzi, acercándose más a la dogmática penal, realiza una clasificación acorde con el bien jurídico tutelado, esta clasificación a diferencia de la realizada por Correa, quien retoma la de Sieber, nos recuerda distintos géneros de bienes jurídicamente tutelados, ahora bien, la novedad consiste eminentemente en el medio que se utiliza para vulnerar los mismos y establece: [95]

Delitos contra el patrimonio;
Delitos contra la intimidad;
Delitos contra la seguridad pública y las comunicaciones;
Falsificaciones informáticas, y
Contenidos ilegales en Internet

Dentro del seno de la Organización de las Naciones Unidas (ONU) se ha realizado un conglomerado de conductas susceptibles de encuadrarse como delitos informáticos, dichas conductas son las siguientes:[96]

Fraudes cometidos mediante manipulación de computadoras;
Manipulación de los datos de entrada;
La manipulación de programas;
Manipulación de los datos de salida;
Falsificación informática;
Daños o modificaciones de programas o datos computarizados;
Sabotaje informático;
Hackers, y

[95] *Ibidem,* p. 28.
[96] *Ibidem,* pp. 29-32.

Reproducción no autorizada de programas informáticos de protección legal

Finalmente, la clasificación del Convenio sobre la ciberdelincuencia del Consejo de Europa (Convención de Budapest) es la siguiente: [97]

> Delitos en contra de la confidencialidad, integridad y disponibilidad de datos y sistemas de cómputo;
> Delitos relacionados con sistemas de cómputo;
> Delitos relacionados con los contenidos; y
> Delitos vinculados a los atentados contra la propiedad intelectual y a los derechos afines

En esta última clasificación podemos observar la precisión con la que se clasifica de forma general a los *ciberdelitos,* clasificación, que a percepción de la autora de esta investigación, es la categorización más adecuada, pues intenta no dejar al margen a ninguna conducta de las cometidas mediante el uso de la tecnología, en ese sentido, como lo veremos en el siguiente tema, uno de los delitos estudiados a precisión y que lesionan gravemente a la sociedad son aquellos que tienen que ver con el contenido que se trasmite.

2.2.5.1. Delitos de Contenido

Dentro de los delitos informáticos de contenido, se hallan los relacionados con las conductas relativas a la pornografía infantil, tema que hace ya varias décadas tiene preocupados a muchos países e incluso se encuentra siempre sobre las mesas de discusión de organismos regionales e internacionales, ya que Internet facilita en gran medida, la distribución y la comercialización de pornografía infantil, cuyos principales afectados son menores de edad.

[97] *http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS_185_spanish.PDF*

De acuerdo con el reporte explicativo del Convenio sobre la ciberdelincuencia del Consejo de Europa, el propósito del artículo 9 tiene como finalidad reforzar las medidas de protección de los menores, incluida su protección contra la explotación sexual, mediante la modernización de las disposiciones del derecho penal con el fin de circunscribir de manera más eficaz la utilización de los sistemas informáticos en relación con la comisión de delitos de índole sexual contra menores. [98]

Este artículo busca castigar tanto la producción, oferta, distribución, posesión y actos de procuración de material pornográfico, a través de sistemas de cómputo, tomando como fundamento y base los instrumentos internacionales más relevantes sobre la materia, tales como el Protocolo Opcional de las Naciones Unidas a la Convención sobre los Derechos del Niño sobre la venta de niños, prostitución infantil y pornografía infantil y la decisión de la Comisión Europea sobre el combate a la explotación sexual de niños y la pornografía infantil. [99]

Considerando la relevancia del tema, vale la pena destacar que el Consejo de Europa introdujo el 25 de octubre de 2007 una Convención sobre la Protección de los Niños en contra de la Explotación Sexual y el Abuso Sexual (Convención CETS no. 201). El principal propósito de esa Convención es prevenir y combatir la explotación y el abuso sexual de niños, proteger los derechos de víctimas de la explotación y el abuso sexual y promover la cooperación nacional e internacional en contra de la explotación y el abuso sexual de los menores. [100]

El artículo 20 de la Convención 201 es similar al artículo 9 de la Convención de Budapest, sin embargo las principales diferencias radican en que la Convención de Budapest está especialmente enfocada a la penalización de actos relacionados con el uso del sistema de cómputo y tecnología de información, mientras que el

---

[98] Reporte explicativo párrafo 91, *http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS%20185%20Explanatory%20report_Spanish.pdf*

[99] Velasco San Martín, Cristos, *op., cit.*, nota 51, p. 65.

[100] *Ibidem*, p. 66.

enfoque de la Convención 201 es mucho más amplio puesto que cubre otras actividades no solamente vinculadas con sistemas de cómputo. Adicionalmente, la Convención 201 sanciona el simple hecho de tener acceso a pornografía infantil, a través de las Tic´s (Tecnologías de la Información y la Comunicaciones) mientras que la Convención de Budapest no sanciona dichas conductas.[101]

2.3. El Convenio sobre ciberdelincuencia del Consejo de Europa (Convenio de Budapest)

2.3.1. Antecedentes

"En 1983 en París la OCDE designó un comité de expertos para discutir el crimen relacionado con las computadoras y la necesidad de cambios en los códigos penales. El dictamen de esta organización, recomendó a los países miembros la modificación de su legislación penal, de forma que se integraran los nuevos delitos informáticos."[102]

"En 1989, el Consejo de Europa convocó a otro comité de expertos, que en la Recomendación emitida el 13 de septiembre de ese año, presentaron una lista mínima de los delitos que debían necesariamente agregarse a las legislaciones de cada país miembro, junto con la lista opcional."[103]

"También se llegó a discutir sobre estos temas en el Décimo Tercer congreso Internacional de la Academia de Derecho Comparado de Montreal en 1990, en el Octavo congreso Criminal de las Naciones Unidas celebrado en el mismo año, y en la conferencia de Wurzgburgo, en Alemania, en 1992."[104]

---

[101] *Idem.*
[102] Cassou Ruíz, Esteban, *op., cit.*, nota 68, p. 226.
[103] *Idem.*
[104] *Idem.*

"El comité Europeo sobre Problemas de Delincuencia (*The European committee on Crime Problems* CDPC) decidió mediante una resolución de Noviembre de 1996 establecer un comité de expertos para tratar aspectos relacionados con el cibercrimen."[105]

> El comité de expertos, conformado celebró 10 sesiones plenarias y 15 reuniones del Grupo Redactor entre Abril de 1997 y Diciembre de 2000, así como 3 reuniones adicionales para finalizar el memorando explicativo. La versión final y revisada del proyecto de Convención y el memorando de referencia, fueron sometidos para su aprobación en junio de 2001 y posteriormente el texto final del proyecto fue enviado al Comité de Ministros para su adopción y para abrirlo a firma entre los países miembros.[106]

2.3.2. Reporte Explicativo

> El Convenio sobre Ciberdelincuencia del Consejo de Europa junto con su Reporte Explicativo fueron adoptados por el Comité de Ministros del Consejo de Europa durante su 109ª Sesión del 8 de noviembre de 2001 y la Convención fue oficialmente abierta para firma en la ciudad de Budapest, Hungría, el 23 de Noviembre de 2001 durante una conferencia internacional sobre cibercrimen.[107]

2.3.3. Objetivos

El Convenio sobre Ciberdelincuencia del Consejo de Europa tiene como objetivos: armonizar los elementos sustantivos de la legislación penal relacionada con disposiciones de cibercrimen; ofrecer las facultades necesarias sobre derecho procedimental doméstico para la investigación y persecución de delitos y otras conductas cometidas a través de sistemas de cómputo y para la obtención de

[105] Velasco San Martín, Cristos, *op., cit.*, nota 51, p. 81.
[106] *Ibidem*, p. 82.
[107] Véase Reporte explicativo párrafo 1

pruebas en relación a la información contenida en forma electrónica y establecer un régimen ágil y efectivo de cooperación internacional, entre otros objetivos.[108]

2.3.4. Países miembros y ratificaciones

El convenio sobre Ciberdelincuencia del Consejo de Europa ha sido firmado por 45 y ratificado por 36 Estados, de los cuales solo 17 Estados Miembros de la Unión Europea lo han ratificado con algunas reservas. Incluso ha sido firmado por países no miembros de la Unión Europea, tal es el caso de Canadá, Japón, Sudáfrica, y los Estados Unidos de América.[109] España ratificó dicho Convenio en el año 2010.

2.3.5. Países Latinoamericanos Miembros

A propósito del tema aduce Cristos Velasco San Martín que:

> Hasta ahora ningún país Latinoamericano ha firmado el Convenio sobre ciberdelincuencia del Consejo de Europa, sin embargo países como Argentina, Colombia y la República Dominicana han aprobado y expedido legislación y reformas a sus marcos jurídicos penales nacionales en materia de ciberdelitos, tomando en cuenta algunas de las disposiciones del Convenio sobre Ciberdelincuencia del Consejo de Europa.
>
> Durante la conferencia Octopus sobre cooperación en contra del cibercrimen llevada a cabo del 23 al 25 de marzo de 2010 en la ciudad de Estrasburgo, el gobierno Argentino expresó formalmente su compromiso de adherirse al Convenio sobre Ciberdelincuencia del Consejo de Europa para poder fomentar la cooperación internacional con otros países.
>
> Es importante señalar, que el Consejo de Europa desde el año 2007 invitó formalmente a los gobiernos de México, Costa Rica y Chile a acceder al protocolo

[108] Véase Reporte explicativo párrafo 16

[109] El documento oficial del Consejo de Europa que contiene la lista oficial de firmas y ratificaciones del Convenio de Budapest al 29 de septiembre de 2014, *http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG*

de adhesión a la Convención. Sin embargo, ninguno de estos países ha ratificado formalmente su compromiso de acceder a dicho protocolo puesto que para ello se requiere previamente de una reforma a los marcos jurídicos penales nacionales tanto sustantivos como procedimentales, así como la creación de CERT's y redes o puntos de contacto 24X7 nacionales para la identificación de conductas penales cometidas a través de Internet.

Vale la pena destacar que el Consejo de Europa está colaborando activamente con la Organización de los Estados Americanos en la promoción de la Convención para que los países latinoamericanos puedan utilizarla como ley modelo, para promover la cooperación internacional y adoptar las mejores prácticas e identificar las problemáticas que tienen otros países relacionados en la lucha contra el cibercrimen.

Precisamente para promover el acceso al Convenio sobre Ciberdelincuencia entre los países latinoamericanos, el Consejo de Europa junto con el Consejo Nacional de Seguridad de México y la Secretaría de Gobernación organizaron un taller regional del 25 al 27 de agosto de 2010 en la ciudad de México donde participaron representantes y expertos de Argentina, Colombia, Chile, Costa Rica, Paraguay, Perú y México. El propósito de este taller regional fue: acelerar y reforzar el proceso de reforma de los marcos jurídicos sustantivos y procesales en materia de ciberdelito conforme a las disposiciones del Convenio sobre ciberdelincuencia; promover y fomentar el acceso y ratificación a este tratado internacional y mejorar la cooperación regional e internacional en materia de ciberdelito conforme a las disposiciones que prevé dicho convenio.[110]

Bajo el auspicio del Gobierno de México y del Consejo de Europa, del 31 de marzo al 2 de abril de 2014 tuvo lugar en la Ciudad de México el "Taller sobre legislación en materia de ciberdelincuencia en América Latina". El propósito del taller consistió en apoyar los procesos de armonización de la legislación y de adhesión al Convenio del Consejo de Europa sobre la Ciberdelincuencia (Budapest, 2001; Serie de

[110] Velasco San Martín, Cristos, *op., cit.*, nota 51, pp. 84-85

Tratados Europeos no. 185), por los países de América Latina que han sido invitados a adherirse, que han manifestado su interés en este sentido, o que ya son Parte.

Todos los países invitados al evento -Argentina, Chile, Colombia, Costa Rica, Panamá, Paraguay, Perú y República Dominicana- respondieron positivamente, con el envío de representantes primordialmente de los ministerios de relaciones exteriores, justicia, y/o ciencia y tecnología, así como de las fiscalías especializadas en la materia. Se sumaron asimismo altas autoridades de la Secretaría de Seguridad Multidimensional de la Organización de los Estados Americanos (OEA) y expertos tanto del Departamento de Justicia de los Estados Unidos como del Consejo de Europa.

Es de observarse que se pretende una unificación, digamos una sintonía unísona para que los países que han sido invitados a formar parte de este Convenio, se adhieran a él. En América, como se ha venido manifestando falta mucho por hacer, por principio de cuentas si el Estado Mexicano pretende incluirse necesita con carácter de urgente y antes que nada una reforma al marco legal penal.

2.4. Elementos de combate a los denominados *ciberdelitos*

2.4.1. Centros de respuesta a Emergencias de Cómputo (CERT's)

Los Centros de Respuesta a Emergencias de Cómputo, mejor conocidos por sus siglas en inglés como CERT's tienen como función principal monitorear la seguridad de las redes y sistemas de información con el objeto de coordinar, facilitar y ofrecer servicios de respuesta inmediata tanto a víctimas de delitos como a organizaciones e instituciones encargadas de la administración y control de sistemas de seguridad y cómputo.

Los CERT's juegan un papel fundamental en la identificación de nuevas amenazas y sirven no solamente como un conducto para facilitar información para la prevención y resolución de incidencias y problemas derivados de ataques

informáticos por conductos tales como el *spam, phishing, malware,* virus *y troyanos*, entre otros, sino que también sirven como un punto nacional de contacto para la coordinación de respuestas y estrategias relacionadas con la seguridad de las tecnologías de información.

Actualmente existen más de 250 CERT's oficialmente reconocidos a nivel mundial. De entre los países latinoamericanos, únicamente Chile, Brasil, Argentina y México tienen CERT's debidamente conformados y oficialmente reconocidos.

Vale la pena destacar que el UNAM-CERT fue oficialmente reconocido en 2001 para operar como tal por el Comité directivo del Foro de Repuesta a Incidentes y Equipos de Seguridad (*Steering Committe of the Forum of Incident Response and Security Teams)*.

El UNAM-CERT funciona como un centro de investigación para diseminar información, proporcionar asesoría y servicios de seguridad, así como para intercambiar experiencias y puntos de vista en torno a políticas de seguridad de sistemas de información y cómputo para ayudar a disminuir la cantidad y gravedad de los problemas de seguridad, así como para difundir una cultura de la seguridad en cómputo en México. [111]

2.4.2. Redes de contacto 24x7

El Grupo de los 8 (G-8) en cuyos orígenes formaban parte sólo 8 países, de ahí su nombre y actualmente lo integran 48 países, tiene conformada una red de puntos de contacto 24X7 desde el año de 1997. El artículo 35 del Convenio sobre Cibercriminalidad del Consejo de Europa establece la necesidad de crear una red de puntos o autoridades de contacto disponibles las 24 horas, los 7 días de la

[111] *Ibidem,* p. 369.

semana con el objeto de facilitar la cooperación internacional para la identificación de los delitos cometidos en la red.[112]

La creación de redes o puntos operativos de contacto 24x7 forma parte de una estrategia para poder identificar, prevenir y facilitar asistencia técnica y jurídica en la identificación y combate de conductas ilícitas cometidas a través de sistemas de cómputo e Internet. De tal suerte que, como se ha visto en esta investigación, para que los países puedan firmar y ratificar el Convenio sobre Ciberdelincuencia del Consejo de Europa, es menester establecer este tipo de redes, puesto que los expertos han señalado que de esta forma se garantiza que los países puedan responder efectivamente a los retos que plantea a las autoridades ejecutoras perseguir los delitos.

El artículo 35 del Convenio sobre Ciberdelincuencia establece:

Artículo 35 - Red 24/7

1. *Cada Parte designará un punto de contacto disponible las veinticuatro horas del día, siete días a la semana, con objeto de garantizar la prestación de ayuda inmediata para los fines de las investigaciones o procedimientos relacionados con delitos vinculados a sistemas y datos informáticos, o para la obtención de pruebas electrónicas de un delito. Dicha asistencia incluirá los actos tendentes a facilitar las siguientes medidas o su adopción directa, cuando lo permitan la legislación y la práctica internas:*

a) *El asesoramiento técnico;*

b) *La conservación de datos en aplicación de los artículos 29 y 30;*

c) *La obtención de pruebas, el suministro de información jurídica y la localización de sospechosos.*

2. *a) El punto de contacto de una Parte estará capacitado para mantener comunicaciones con el punto de contacto de otra Parte con carácter urgente.*

b) Si el punto de contacto designado por una Parte no depende de la autoridad o de las autoridades de dicha Parte responsables de la asistencia mutua

[112] *http://ciberdelincuencia.org/fuentes/organizaciones.php*

internacional o de la extradición, el punto de contacto velará por garantizar la coordinación con dicha autoridad o autoridades con carácter urgente.

3. Cada Parte garantizará la disponibilidad de personal debidamente formado y equipado con objeto de facilitar el funcionamiento de la red.

Cada país tendrá la libertad de determinar el lugar donde deberá ubicarse el punto de contacto dentro de su estructura gubernamental y de conformidad con su propio sistema jurídico. Es importante que la red de contacto cuente con equipo y tecnologías necesarias para su correcto funcionamiento, lo anterior con la finalidad de detectar a tiempo las amenazas y poder compartir información de utilidad con otros miembros de la red en contacto.

2.4.3. Red de Contacto de INTERPOL

"INTERPOL (policía internacional) ha desarrollado un sistema mundial de comunicación policial conocido como I-24/7 para permitir a los cuerpos policiacos, comunicarse de forma segura en todo el mundo."[113] El sistema tiene la finalidad de conectar entre sí a los funcionarios encargados de la aplicación de la ley de todos los países miembros, lo que permite a los usuarios autorizados intercambiar información policial vital y acceder a las bases de datos y a los servicios de INTERPOL 24 horas al día.[114]

Esta red a los investigadores acceder a los instrumentos de tecnología de punta de INTERPOL y establecer conexiones entre segmentos de información aparentemente inconexos, lo que facilita las investigaciones y ayuda a resolver los casos. En la actualidad todos los países que son miembros de INTERPOL, están conectados y su principal objetivo al participar, es la utilización de la red para investigar los delitos cibernéticos.[115]

---

[113] Velasco San Martín, Cristos, *op., cit.*, nota 51, p. 158.
[114] *http://www.interpol.int/es/INTERPOL-expertise/Data-exchange/I-24-7*
[115] *Idem.*

En cuestión de segundos, los usuarios autorizados pueden buscar y cotejar información gracias al acceso directo a las bases de datos sobre presuntos delincuentes o personas buscadas por la justicia, documentos de viaje robados y perdidos, vehículos robados, huellas dactilares, perfiles de ADN y documentos administrativos robados y obras de arte robadas. [116]

[116] *Idem.*

CAPÍTULO 3. DE LA INVESTIGACIÓN DE LA POLICÍA EN LOS DENOMINADOS CIBERDELITOS

3.1. Cibercrimen

El autor de origen español Fernando Miró Llinares, aduce que la terminología utilizada recientemente para referirnos a los delitos informáticos, se ha visto influenciada por aportaciones al tema del país de habla inglesa más importante del mundo y así refiere:

> En los últimos tiempos se ha venido sustituyendo, aunque no por todos, la denominación de los delitos informáticos por la de cibercrimen y cibercriminalidad en referencia esta vez al termino anglosajón, *cybercrime,* procedente 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
>
> A partir del nuevo siglo empezaron a preocupar ya no solo 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 personal o la propia seguridad nacional. Y todo ello ha llevado a la utilización de un término, el de *cibercrimen* que, a mi parecer, logra englobar todas las tipologías de comportamientos que deben estar, y además alcanza mejor que otros el que debe ser el propósito esencial de cualquier concepto que sirve para nombrar una categoría: enfatizar aquello que une a todo lo que la conforma que, en este caso, es Internet y las Tecnologías de la Información y la Comunicación, como medio de comisión delictiva.[117]

[117] Miró Llinares, Fernando, *El cibercrimen, fenomenología y criminología de la delincuencia en el ciberespacio,* Madrid, Marcial Pons, 2012, pp. 37-39

Sin embargo, no es novedoso para nadie, que a partir de los atentados en New York el 11 de septiembre de 2001, el gobierno de Estados Unidos, se dedicó a realizar una caza interminable contra grupos de terroristas que, valiéndose de la tecnología, lograron perpetrar y vulnerar la seguridad de lo que hasta entonces se conocía como el Estado más seguro de este planeta. A partir de ese momento, comenzaría el auge de lo que hoy conocemos como: *el cybercrimen.*

3.2. El ciberdelincuente

Por principio de cuentas, entiéndase quienes son los delincuentes cibernéticos o ciberdelincuentes, ya que no son sólo aquellos que cometen delitos informáticos, sino más aún: "Son aquellos que cometen una conducta antijurídica, antisocial, típica, culpable y punible, valiéndose de las nuevas tecnologías mediante cierto grado de conocimiento de la informática". [118]

Ahora bien, para efectos de la presente investigación, obsérvese como un delincuente actúa en los ciberdelitos y cuya peligrosidad se incrementa, en razón de ser más difíciles de perseguir:

> Suele enmascararse bajo identidades ficticias, apodos o *nicks,* suplantaciones de personalidades, etcétera, esto es, suele tratar de permanecer anónimo (*proxys,* servidores de correo web, *anonimizadores* web), y difunde sus ilícitos (en audio, vídeo o datos) a través de la red usando *remailers,* aprovechándose de la trasnacionalidad al ciberespacio, a través de servidores interpuestos en el territorio de diferentes países, de modo y manera que es a veces muy difícil, si no imposible, averiguar con certeza la fuente o punto de origen del ilícito y las intermediaciones entre el remitente y el destinatario final de las comunicaciones electrónicas, y cuando se localizan geográficamente, su autor ya no suele encontrarse en ese punto o se descubre que lo ha hecho desde ubicaciones de usuarios públicos de imposible

[118] Vázquez Azuara, Carlos Antonio, *op., cit.,* nota 65, p.126.

singularización (cibercafés, ciberbibliotecas, redes, cibercentros, sin identificación de usuarios)[119]

A medida que avanza el tiempo se ve mucho más lejana la posibilidad de, ya no superar, sino más bien alcanzar la legalidad de algunas conductas que se realizan mediante el uso de la tecnología y el castigo para aquellas que se consideren socialmente reprobables.

3.2.1. El uso de la red para cooptar víctimas

"A la primera generación de la cibercriminalidad en la que lo característico era el uso de ordenadores para la comisión de delitos, le ha sucedido una segunda época en la que la característica central es que el delito se comete a través de Internet"[120]

> Puede parecer que el uso de la red para encontrar a las víctimas de un crimen hace de ella una herramienta del crimen. En algunos casos, el criminal utiliza Internet para cometer el crimen (por ejemplo, enviar cartas electrónicas en cadena, enviar por correo electrónico noticias falsas de ISP[121] de la víctima pidiendo información de su tarjeta de crédito o dirigiendo a las víctimas que intentan venderles productos bajo falsos pretextos). En todos estos casos Internet es una herramienta del crimen, pero el acto inicial de buscar a la víctima no es, en sí mismo, criminal.[122]

Visto lo anterior, ahora podemos señalar en un segundo plano la situación en la que Internet permite asechar a las víctimas, sólo eso, hallarlas así tenemos que es el medio ideal para que, por ejemplo, un pedófilo, violador o tratante de blancas,

---

[119] Velasco Núñez, Eloy, *Delitos cometidos a través de internet, cuestiones procesales,* Madrid, Ed. La Ley 2010, p. 77

[120] Miró Llinares, Fernando, *op., cit.,* nota 117, p. 37.

[121] ISP son las siglas de *Internet Service Provider* Proveedor de Servicios de Internet**,** una compañía que proporciona acceso a Internet. Por una cuota mensual, el proveedor del servicio te da un paquete de software, un nombre de usuario, una contraseña y un número de teléfono de acceso. A través de un módem (a veces proporcionado también por el ISP), puedes entonces entrar a Internet y navegar por el World Wide Web, el USENET, y enviar y recibir correo electrónico.

[122] Nava Garcés, Alberto Enrique, *op., cit.*, nota 55, p. 12.

encuentre el perfil perfecto de su víctima y luego cometa el crimen en el mundo real, no así en el ciberespacio o el mundo virtual, como lo conocemos y hemos analizado en un primer momento. Es decir, los criminales en el mundo real están valiéndose de Internet circunstancialmente para sus delitos.

3.2.2. El uso de redes sociales

A últimas fechas se ha vuelto tan común, como normal escuchar hablar a las personas a cerca de las redes sociales, en los medios de comunicación, en las noticias e incluso dicho término es motivo de utilización por los miembros de una familia en una conversación usual, sin embargo al preguntarnos que son las redes sociales podemos observar la siguiente acepción:

> Una red social, a nivel general, es una estructura social formada por nodos habitualmente individuos u organizaciones que están vinculados por uno o más tipos de interdependencia, tales como valores, puntos de vista, ideas, intercambio financiero, amistad, parentesco, conflicto, comercio, entre otras. Las estructuras resultantes usualmente son muy complejas. [123]

De lo anterior se advierte que las redes sociales pueden considerarse como un sistema que, como cualquier otro, a su funcionamiento, va a mostrar un resultado, en este caso se hará posible establecer relaciones con otras personas indiscriminadamente, intercambiar información, como datos, imágenes, sitios, música, videos, etcétera.

3.2.2.1. Principales redes sociales

La Asociación Mexicana de Internet (AMIPCI) ha realizado en dos ocasiones un estudio sobre Redes Sociales, el último de los mismos se ha denominado *MKT Digital y Redes Sociales en México 2013*. La encuesta fue aplicada a 5 199

[123] Valenzuela Argüelles, Rebeca, "Las redes sociales y su aplicación en la educación*", Revista Digital Universitaria,* México, volumen 14, núm. 4, 1 de abril de 2013, p. 7.

internautas mexicanos pertenecientes a todos los rangos de edad y niveles socioeconómicos del universo total de internautas en México.[124]

Sólo el 7% de las personas entrevistadas indicó que no usa redes sociales, de ese porcentaje, la mayoría lo considera así, el 35% desea proteger sus datos, el 24% las canceló, el 18% simplemente no le es de interés, el 15% no tiene tiempo, el 6% no las utiliza por miedo a engancharse y solo el 2% no sabe cómo funcionan. La generalidad de usuarios está en un rango de 3 a más de 5 años de uso de redes sociales. Así 9 de cada 10 internautas acceden a una red social.[125]

Facebook es la red que más acceso tiene con un 96% de usuarios mexicanos inscritos, quienes en su mayoría son de 18 a 24 años de edad. Después está *Twitter* con un 69%. Luego tenemos a *Youtube*, con un 65%. Finalmente *Google* + con un 57%, y la mayoría en el rango de 18 a 24 años.[126]

Las anteriores estadísticas, realizadas en el año de 2013, muestran que Facebook es la red que más acceso tiene por parte de los mexicanos, el llamado por muchos "*libro de las caritas"*, por su traducción al español, se ha convertido en un medio ideal para que los criminales contacten a sus víctimas en el mundo virtual y de esta manera lleguen a cometer delitos en su contra en el mundo real, esto ocurre porque las personas tienden a colocar en estos espacios, información relativa a su nivel de vida sin limitar el acceso a la información.

Aunque la mayor parte del tiempo el modo de operar del delincuente en algunos delitos sigue siendo el tradicional, es decir, el de seguir de cerca a la víctima y analizar su vida rutinaria, como en el caso preciso del delito de secuestro, el problema se presenta cuando sin restricción, cualquiera puede ver la vida de las

[124] *https://www.amipci.org.mx/estudios/otros_estudios/MKT_Digital_y_Redes_Sociales_en_M%C3%A9xico_2013.pdf*

[125] *Idem.*

[126] *Idem.*

personas. Así va siendo cada vez más común encontrar casos en los que mediante el uso de esta red social se comenten crímenes.[127]

3.3. Análisis a la legislación mexicana aplicable a los ciberdelitos

Las etapas en las que se funda la existencia de un ciberdelito son tres: la de inclusión en los catálogos penales (legislación) la forma en que se debe investigar (forense informática) y la forma en que se acredita ante un juzgado o tribunal (prueba electrónica). Los mexicanos aún nos encontramos con las dificultades que implica la primera.[128]

3.3.1. Códigos Penal Federal y Código Nacional de Procedimientos Penales

En México no existe una legislación específica que sancione y castigue los ciberdelitos; empero, el Código Penal Federal vigente y otras leyes a nivel federal y estatal establecen y castigan algunas conductas cometidas a través de sistemas de cómputo o a través del uso de sistemas o equipos informáticos.[129]

Así tenemos, ejemplificando, que el Código Penal Federal estable respecto de las sanciones a quienes cometan una conducta relacionada con los *ciberdelitos* en su Título Noveno, Capítulo II, artículos 211 bis 1 a 211 bis 7, a decir del análisis de Cristos Velasco:

---

[127] Obsérvese los encabezados de las siguientes noticias: 14 de mayo de 2014.- Tijuana, México.- Dos jóvenes de 18 y 19 años de edad, fueron detenidas por elementos de la Procuraduría de Justicia de Baja California, como presuntas responsables de encabezar una red de secuestro que contactaba a sus víctimas vía Facebook, disponible en: *http://www.excelsior.com.mx/nacional/2014/05/14/959260#imagen-1.* 23 de abril de 2013.- San Luis Potosí, México.- Brenda Guadalupe Tristán Rodríguez, de 17 años, se convirtió en otra víctima de las redes sociales al trabar amistad con Érick Darío Salas Valencia, de 18, quien después de un tiempo la secuestró y la asesino, disponible en: *http://www.proceso.com.mx/?p=339886*

[128] Nava Garcés, Alberto Enrique, *op., cit.*, nota 55, p. 122.

[129] Velasco San Martín, Cristos, *op., cit.*, nota 51, p. 299.

> Penas de prisión que van de seis meses a ocho años de prisión y sanciones económicas a quien copie información, modifique, destruya o provoque pérdida de información contenida tanto en sistemas o equipos de informática del Estado o medios de almacenamiento informáticos de seguridad pública o en sistemas o equipos de informática de las instituciones que integran el sistema financiero.[130]

No obstante lo anterior, como antecedentes hallamos que en 1999, cuando el Código Penal Federal regía en el Distrito Federal para los delitos del fuero común se incluyó el catálogo de delitos, al hablarse de Distrito Federal, debe quedar claro que es refiere a solo a los delitos del fuero común, bajo el rubro *Revelación de secretos y acceso ilícito a sistemas y equipos de informática*, el cual está expresado en los artículos 211 bis 1 al 211 bis 7, de dicho código.[131]

Finalmente, por cuanto hace a este efecto, en el año de 2002, cuando se publicó el entonces Nuevo Código Penal para el Distrito Federal, que: "Entre cuyas características destacó la ausencia de legislación en materia de informática, con la salvedad del artículo 231, fracciones XVI, que hace referencias a transferencia por medio electrónico".[132]

En la actualidad, respecto a las legislaciones de los Estados y por cuanto hace a los delitos informáticos, tenemos que los Códigos Penales de Aguas Calientes, Durango y Tabasco establecen dichas figuras entre los delitos contra la seguridad en los medios informáticos y magnéticos; Baja California los establece en los delitos contra la inviolabilidad del secreto; Chiapas en los delitos en contra de las personas en su patrimonio, Colima, Puebla, Querétaro, Zacatecas y Morelos, en los delitos contra la moral pública y en los delitos contra la libertad y la violación de otras garantías y Tamaulipas, Quintana Roo, Michoacán y Coahuila en los delitos revelación de secretos y de acceso ilícito a sistemas y equipos de informática.

---

[130] *Idem.*
[131] Nava Garcés, Alberto Enrique, *op., cit.*, nota 55, pp. 122-123
[132] *Idem.*

Sin embargo en los Estados de Baja California Sur, Campeche, Estado de México, Guanajuato, Guerrero, Hidalgo, Jalisco, Nayarit, Nuevo León, San Luis Potosí, Sonora, Tlaxcala, Veracruz y Yucatán, no se contiene disposición relativa sobre el particular en los delitos tipificados en sus códigos penales.

Siguiendo el mismo orden de ideas, nos referimos ahora a la legislación procesal penal mexicana, esto es, el Código Nacional de Procedimientos Penales, mismoque no hace referencia a la persecución de conductas cometidas a través de sistemas de cómputo e informáticos, por tanto tampoco específica que autoridades y tribunales deberían ser competentes para investigar, procesar y castigar conductas cometidas a través de sistemas de cómputo e Internet, y por ende, no se establecen procedimientos de cooperación y coordinación entre cuerpos policíacos, el Ministerio Público y los Jueces o Tribunales del Poder Judicial que son parte esencial en cualquier procedimiento.[133]

Más aun, el Nuevo Código Nacional de Procedimientos Penales, publicado en el Diario Oficial de la Federación el 5 de marzo de 2014, no expresa la forma de investigar, procesar y sancionar el tipo de delitos materia de esta investigación. Pese a que se trata de una propuesta ambiciosa de inclusión de las Entidades Federativas y máxime con la aplicación del sistema penal acusatorio adversarial, es casi nula la propuesta del legislador para la regulación de los delitos informáticos (ciberdelitos). Únicamente se ha incluido un tema en cuanto a *"la intervención de las comunicaciones privadas".* Obsérvese el contenido del artículo 291, que a la letra dice:

> ***Artículo 291. Intervención de las comunicaciones privadas***
> *Cuando en la investigación el Ministerio Público considere necesaria la intervención de comunicaciones privadas el Titular de la Procuraduría General de la República o los servidores públicos facultados en términos de su ley orgánica, así como los Procuradores de las Entidades federativas, podrán solicitar al Juez federal de control*

[133] Velasco San Martín, Cristos, *op., cit.*, nota 51, p. 299

competente, por cualquier medio, la autorización para practicar la intervención, expresando el objeto y necesidad de la misma.

La intervención de comunicaciones privadas, abarca todo un sistema de comunicación, o programas que sean fruto de la evolución tecnológica, que permitan el intercambio de datos, informaciones, audio, video, mensajes, así como archivos electrónicos, que graben, conserven el contenido de las conversaciones o registren datos que identifiquen la comunicación, las cuales se pueden presentar en tiempo real o con posterioridad al momento en que se produce el proceso comunicativo.

Empero, dicho artículo, como se verá más adelante en la actividad probatoria, es motivo de innumerables cuestionamientos, ya que por su naturaleza procesal y la relevancia del tema, podría pensarse violatorio de garantías individuales. En este momento sería prematuro pronunciarse al respecto, aun cuando es un tema que se encuentra desde hace varios años en la mesa de discusiones de aquellos que tienen la facultad para emitir resoluciones judiciales.

La situación hace que en la práctica se vuelva mucho más complicado poder perseguir y procesar delitos informáticos puesto que no existen disposiciones específicas que describan, atribuyan y delimiten la competencia en materia de investigación, persecución y procesamiento de conductas delictivas cometidas a través de sistemas de cómputo e Internet a los órganos antes señalados.

3.3.2. Jurisprudencia

Recuérdese que la jurisprudencia es importante en cuanto a que en el orden jurídico subsana las imperfecciones que pudiesen darse, creando contenidos jurídicos para casos futuros similares, que si bien no serán iguales, pueden tener un parecido sustancial. Luego entonces, siempre que nos encontramos frente a una ausencia legislativa, una laguna dentro del derecho que por su naturaleza no pueda ser resuelta en el ámbito común, normalmente se pretende echar mano del Código Penal Federal, que revela que un determinado número de artículos, que si bien no

son específicamente relativos a los delitos informáticos, cuando menos hay un contenido de ellos, así las autoridades lo han hecho extensivo, volviéndolo competencia del fuero Federal; sin embargo, ya la Suprema Corte de Justicia de la Nación (SCJN) se ha pronunciado sobre el particular advirtiendo la incompetencia en que incurren los Agentes del Ministerio Público de la Federación o los Tribunales cuando el afectado no cumple con las hipótesis contenidas en el artículo 50 de la Ley Orgánica del Poder Judicial de la Federación.[134]

Para tal efecto, lo analizaremos desde el punto de vista jurisprudencial, cuando de competencia penal se trata:

> ***COMPETENCIA PENAL. AUN CUANDO NO SE HUBIERE PLANTEADO CORRECTAMENTE, PROCEDE RESOLVERLA.***
>
> *Las cuestiones de competencia son de interés general, se rigen por el derecho público que reglamenta el orden general del Estado en sus relaciones con los gobernados, los demás Estados y cuando son entre autoridades judiciales se traduce en un reflejo de los atributos de decisión e imperio de que están investidas, por lo que no debe existir tardanza en establecer en qué fuero radica o a qué juzgador corresponde el conocimiento de determinada causa penal. Esta Primera Sala de la Suprema Corte de Justicia de la Nación, considera que la decisión de declarar la inexistencia del conflicto competencial, cuando alguna autoridad judicial no se pronunció sobre si es o no competente para conocer de una causa penal, o de ordenar la reposición del procedimiento, cuando no se siguieron las formas previstas para el planteamiento del conflicto produciría demora injustificada en perjuicio del interés general, del ofendido y del probable responsable, tal criterio debe aplicarse en los casos en que obran en el expediente los elementos suficientes para dictar la resolución correspondiente y no hubiere duda para establecer el fuero en que radica la competencia, así como al órgano juzgador que corresponda su conocimiento, atendiendo a las reglas respectivas; en cambio, no es aplicable ese criterio en aquellos procesos penales en que exista duda sobre la determinación de*

[134] Nava Garcés, Alberto Enrique, *op., cit.*, nota 55, pp. 123

la competencia, ya que ocasionaría el efecto contrario al que se pretende, porque retardaría la decisión que debe emitirse sobre el particular.

<u>COMPETENCIA 157/98.</u> Suscitada entre el Juez Décimo Segundo de Distrito en Materia Penal en el Distrito Federal, el Juez Vigésimo Segundo Penal del Distrito Federal y el Juez Primero Penal de Primera Instancia del Sexto Distrito Judicial del Estado de Morelos. 1o. de julio de 1998. Cinco votos. Ponente: Juan N. Silva Meza. Secretaria: Guillermina Coutiño Mata.

Competencia 124/98. Suscitada entre el Juez Primero de Distrito en el Estado de Sinaloa y el Juez Tercero de Distrito en Materia Penal en el Distrito Federal. 14 de octubre de 1998. Unanimidad de cuatro votos. Ausente: Juan N. Silva Meza. Ponente: Olga Sánchez Cordero de García Villegas. Secretario: Jorge Carreón Hurtado. Competencia 427/98. Suscitada entre el Juez Segundo Penal en el Estado de Aguascalientes y la Juez Vigésimo Octavo Penal en el Distrito Federal. 4 de noviembre de 1998. Unanimidad de cuatro votos. Ausente: Juan N. Silva Meza. Ponente: José de Jesús Gudiño Pelayo. Secretario: Ismael Mancera Patiño. Competencia 158/99.

Suscitada entre el Juez de lo Penal del Distrito Judicial de Chiautla de Tapia y el Juez Cuarto de Distrito, ambos en el Estado de Puebla. 26 de mayo de 1999. Unanimidad de cuatro votos. Ausente: José de Jesús Gudiño Pelayo. Ponente: Humberto Román Palacios. Secretario: Miguel Ángel Zelonka Vela.Competencia 288/99.

Suscitada entre el Juez Primero Penal de Primera Instancia del Distrito Judicial de Uruapan, Michoacán y el Juez Cuadragésimo Noveno Penal en el Distrito Federal. 25 de agosto de 1999. Cinco votos. Ponente: Juventino V. Castro y Castro. Secretaria: Rosalba Rodríguez Mireles.

Tesis de jurisprudencia 3/2000. Aprobada por la Primera Sala de este Alto Tribunal, en sesión de primero de marzo de dos mil, por unanimidad de cinco votos de los señores Ministros: presidente José de Jesús Gudiño Pelayo, Juventino V. Castro y

Castro, Humberto Román Palacios, Juan N. Silva Meza y Olga Sánchez Cordero de García Villegas.[135]

Se advierte entonces que la competencia penal, cuando de delito informático se trata, sí la conducta se despliega en el ámbito local no puede ser trasladada al federal, intentando aplicar el Código Penal Federal, pues no procede ser resuelta *en aquellos procesos penales en que exista duda sobre la determinación de la competencia, ya que ocasionaría el efecto contrario al que se pretende, porque retardaría la decisión que debe emitirse* y basta decir que dentro de las facultades que se les otorgan a los Jueces Federales no existe aquella que le permita conocer de hechos ocurridos entre particulares, cuya calidad de sujetos activos o pasivos no pertenece al ámbito Federal.

Por tanto, los delitos informáticos, son materia de la legislación local o bien, del Distrito Federal, por lo que su ausencia (cuando se trata de particulares) afectará sólo a los particulares y no a la Federación. Y si los particulares recurren a la instancia Federal entonces no prospera su acusación, en virtud de que ni el Agente del Ministerio Público Federal, ni el Juez Federal, serán competentes para conocer del asunto.

Es evidente que esta laguna jurídica no puede ser subsanada incluso por los pronunciamientos de la SCJN, así como lo es que trae aparejada serias limitantes y obstáculos para la *investigación* y persecución de ciberdelitos puesto que en una investigación penal de esta naturaleza están involucradas distintas partes, por un lado el CERT nacional, los cuerpos policíacos a nivel Federal y Estatal, la policía cibernética, el Ministerio Público y los Jueces y Magistrados a nivel Federal y Estatal encargados de juzgar los delitos.

[135] Tesis: 1a./J. 3/2000 *Semanario Judicial de la Federación y su Gaceta,* Novena Época, Primera Sala, t. XI, marzo de 2000, p. 119.

3.4. Problemáticas en la investigación de los ciberdelitos en México

Es una realidad que la invasión de la tecnología como elemento en la comisión de hechos delictivos, tenía que demandar cambios, principalmente en la forma de investigación de dichos ilícitos. Tomando en consideración que a la forma de investigar estos delitos se puede entender como la forense informática y para el éxito de la investigación se requiere de peritos en la materia.

En este sentido, si bien es cierto que las conductas ilícitas pueden en algunos casos, permanecer inalteradas en los que respecta a su tipología, la utilización de sistemas de información permite la comisión de las mismas en forma remota en una situación de relativo anonimato, multiplicando al mismo tiempo los efectos tanto en el territorio como en el número de víctimas en forma teóricamente ilimitada. Frente a esta realidad, cualquier investigación penal sobre el tema se encontrará con desafíos y ante la falta de legislación, las autoridades investigadoras tendrán que trabajar con las pocas herramientas que tienen.[136]

Para llevar a cabo la actividad probatoria de los delitos informáticos es necesario que, las autoridades que estuvieron encargadas de la investigación cuenten con un entrenamiento especializado, pues dicha acción implica acceder a constancias que, por su naturaleza, resultan de difícil comprensión para quien desconoce del tema.

3.4.1. La actividad probatoria en los ciberdelitos

Como ya se ha mencionado en párrafos anteriores de esta investigación, es indispensable para intervenir un correo electrónico, realizar el análisis de la superficie de disco, intervención de ordenadores, etcétera., es necesario un perito experto en la materia. Sin embargo ello, por sí solo, no implica una diferenciación

[136] Iglesias, Gonzalo, “El problema de la investigación de los delitos informáticos”, *Revista Digital de la Red Iberoamericana de Derecho informático,* Argentina, núm. 13, diciembre de 2012, p. 16.

con otros medios probatorios como la química, por nombrar alguna. El problema es que al mismo tiempo, la prueba informática presenta particularidades que hacen necesaria la especialización de quien persigue, tanto como de quien juzga.

Por principio de cuentas, debemos mencionar que la prueba informática es, en esencia, volátil. Aun los soportes pensados para almacenamiento, como los discos rígidos son modificables y se degradan con el tiempo y el uso, circunstancia que hace necesario un particular celo en la conservación de la prueba y su cadena probatoria, dicho sea de paso, debe ser por un grupo de expertos en la materia que cuenten los conocimientos técnicos suficientes para preservar la evidencia digital durante el tiempo que sea necesario y útil.

3.4.1.1. La prueba electrónica

En palabras del autor español Eduardo de Urbano, la prueba electrónica: "Se trata de un documento electrónico concebido por una voluntad humana".[137] Pero aun cuando requiera un medio de perfeccionamiento, indica dicho autor, deberá observar las reglas de desahogo que le correspondan y así entra en el grupo de las que se deben presentar mediante el uso de la tecnología.

La prueba electrónica incluye tanto los dispositivos electrónicos que crean, contienen o reproducen los archivos electrónicos (computadora, teléfono celular, escáner, cámara digital, *usb, skimer,* etcétera.) así como la información (programas de datos, bases de datos, imágenes digitalizadas, correos y mensajes electrónicos, etcétera) contenida o reproducida por estos medios.

La prueba electrónica, para su desahogo necesitará ser impecable (evitar su manipulación) y por supuesto deberá contener todos los elementos que la hacen ser lícita.

[137] Nava Garcés, Alberto Enrique, *op., cit.*, nota 55, p.156.

En tal sentido, indica Gabriel Cámpolli:

> La evidencia digital es muy frágil y puede perderse o modificarse con demasiada facilidad, aun por la simple inacción de quien tiene a cargo el cateo o aseguramiento de los bienes, lo que implica la utilización de medidas especiales para su conservación en estado original para poder ser aportada como prueba válida en cualquier proceso penal.[138]

Así también, aduce dicho autor, que de no hacerse el correcto aseguramiento de lo que él llama bienes electrónicos, con el tiempo sólo logrará que se cause aquel efecto conocido como *el principio de los frutos del árbol de raíces amargas o envenenadas,* nada más y nada menos que la altísima impunidad basada en sentencias que contrarias por el hecho de que sí en un principio o en cualquier parte del procedimiento se aplican o se aportan pruebas, nulas, de dudosa obtención o que afecten garantías individuales, entonces el efecto causado, incluso desde la investigación y al momento de sentenciar, será que se absuelva a partir un haber infringido el debido proceso a partir de pruebas obtenidas al margen de exigencias constitucionales y legales.

3.4.1.2. La intervención de las comunicaciones privadas. ¿Violatorio de garantías?

Ahora bien, bajo siguiendo el orden de ideas, tenemos que la utilización de la prueba electrónica implica la intervención sobre derechos consagrados constitucionalmente como el derecho a la inviolabilidad de las comunicaciones, que podrían atentar contra el derecho a la intimidad. A partir de ello, es necesario diferenciar la posibilidad técnica de obtener una información de su admisibilidad legal, operación que entra claramente en el campo de la ciencia jurídica.

[138] *Ibidem, p*. 164.

Por principio de cuentas, al no haber disposiciones legales que permitan regir las prácticas en el ámbito del uso de la tecnología, el único medio de claridad que se puede obtener, son aquellos pronunciamientos hechos por la Suprema Corte de Justicia de la Nación, e incluso los cuales contienen ciertas contradicciones, como veremos a continuación y que por la naturaleza de las mismas, dificultan la investigación de los delitos. En la siguiente tesis jurisprudencial se indica que bajo ningún motivo el Ministerio Público pueda exigir a los agentes investigadores la reproducción de los archivos electrónicos que contenga el teléfono móvil de un detenido, a saber de:

> ***DERECHO A LA INVIOLABILIDAD DE COMUNICACIONES PRIVADAS. EL HECHO DE QUE EL JUEZ COMPETENTE PUEDA, EXCEPCIONALMENTE, EN LA PERSECUCIÓN E INVESTIGACIÓN DE LOS DELITOS, ORDENAR LA INTROMISIÓN A TELÉFONOS CELULARES, NO IMPLICA QUE EL MINISTERIO PÚBLICO PUEDA EXIGIR A LOS AGENTES INVESTIGADORES LA REPRODUCCIÓN DE LOS ARCHIVOS ELECTRÓNICOS QUE CONTENGA EL TELÉFONO MÓVIL DE UN DETENIDO.***
>
> *El derecho a la privacidad o intimidad está protegido por el artículo 16, párrafo primero, de la Constitución Política de los Estados Unidos Mexicanos, el cual establece la garantía de seguridad jurídica de todo gobernado a no ser molestado en su persona, familia, domicilio, papeles o posesiones, sino cuando medie mandato de autoridad competente debidamente fundado y motivado; además, el párrafo décimo segundo del propio numeral dispone que las comunicaciones privadas son inviolables, pero que el Juez valorará el alcance de éstas, siempre y cuando contengan información relacionada con la comisión de un delito, mientras que el siguiente párrafo establece que exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada y que para ello la autoridad competente deberá fundar y motivar las causas legales de la solicitud, expresando además, el tipo de intervención, los sujetos y su duración, sin que tales autorizaciones puedan otorgarse cuando se trate de materias de carácter electoral, fiscal, mercantil, civil,*

laboral o administrativo, ni en el caso de las comunicaciones del detenido con su defensor. Ahora bien, los archivos electrónicos almacenados en teléfonos celulares merecen la protección que se les otorga a las comunicaciones privadas, ya que actualmente, a través de esos medios, pueden resguardarse datos privados e íntimos de las personas, en forma de texto, audio, imagen o video, los cuales, de revelarse a terceros, pueden llegar a afectar la intimidad y privacidad de alguien, en ocasiones, con mayor gravedad y trascendencia que la intervención a una comunicación verbal o escrita, o incluso a un domicilio particular; luego, no existe razón o disposición constitucional alguna que impida extender la garantía de inviolabilidad de las comunicaciones privadas a los teléfonos celulares que sirven para comunicarse, además de verbalmente, mediante el envío y recepción de mensajes de texto, y de material audiovisual, así como para conservar archivos en los formatos ya referidos y acceder a cuentas personales en Internet, entre otras funciones afines, máxime que la Constitución Federal no limita su tutela a las formas escritas y verbales de comunicación, sino que alude a las comunicaciones privadas en general. Así, tratándose de la persecución e investigación de delitos, excepcionalmente el Juez competente podrá ordenar la intromisión a los teléfonos celulares, pero en ningún caso el Ministerio Público puede exigir a los agentes investigadores que reproduzcan los archivos electrónicos que contenga el teléfono celular de algún detenido.[139]

CUARTO TRIBUNAL COLEGIADO DEL DÉCIMO OCTAVO CIRCUITO.
Amparo directo 241/2010. 7 de julio de 2011. Mayoría de votos. Disidente: Ma. Carmen Pérez Cervantes. Ponente: Gerardo Dávila Gaona. Secretario: Max Gutiérrez León.

Por fortuna de las autoridades investigadoras del delito esta tesis ha sido superada por *contradicción de tesis 194/2012*, *de la que derivó la tesis jurisprudencial 1a./J. 115/2012 (10a.)* donde se establece que para intervenir una

[139] Tesis: XVIII.4o.7 P (9a.), *Semanario Judicial de la Federación y su Gaceta* Décima Época, t. 2, marzo de 2012, p. 1125.

comunicación privada se requiere autorización exclusiva de la *autoridad judicial federal*, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, y que a la letra dice:

DERECHO A LA INVIOLABILIDAD DE LAS COMUNICACIONES PRIVADAS. SU ÁMBITO DE PROTECCIÓN SE EXTIENDE A LOS DATOS ALMACENADOS EN EL TELÉFONO MÓVIL ASEGURADO A UNA PERSONA DETENIDA Y SUJETA A INVESTIGACIÓN POR LA POSIBLE COMISIÓN DE UN DELITO.

En términos del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, para intervenir una comunicación privada se requiere autorización exclusiva de la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, por lo que todas las formas existentes de comunicación y las que son fruto de la evolución tecnológica deben protegerse por el derecho fundamental a su inviolabilidad, como sucede con el teléfono móvil en el que se guarda información clasificada como privada por la Primera Sala de la Suprema Corte de Justicia de la Nación; de ahí que el ámbito de protección del derecho a la inviolabilidad de las comunicaciones privadas se extiende a los datos almacenados en tal dispositivo, ya sea en forma de texto, audio, imagen o video. Por lo anterior, no existe razón para restringir ese derecho a cualquier persona por la sola circunstancia de haber sido detenida y estar sujeta a investigación por la posible comisión de un delito, de manera que si la autoridad encargada de la investigación, al detenerla, advierte que trae consigo un teléfono móvil, está facultada para decretar su aseguramiento y solicitar a la autoridad judicial la intervención de las comunicaciones privadas conforme al citado artículo 16 constitucional; sin embargo, si se realiza esa actividad sin autorización judicial, cualquier prueba que se extraiga, o bien, la que derive de ésta, será considerada como ilícita y no tendrá valor jurídico alguno

CONTRADICCIÓN DE TESIS 194/2012. Entre las sustentadas por el Segundo Tribunal Colegiado en Materias Penal y Administrativa del Décimo Séptimo Circuito y el Cuarto Tribunal Colegiado del Décimo Octavo Circuito. 10 de octubre de 2012.

La votación se dividió en dos partes: mayoría de cuatro votos por lo que se refiere a la competencia. Disidente: José Ramón Cossío Díaz. Unanimidad de cinco votos en cuanto al fondo. Ponente: Guillermo I. Ortiz Mayagoitia. Secretario: Jorge Antonio Medina Gaona.

Tesis de jurisprudencia 115/2012 (10a.). Aprobada por la Primera Sala de este Alto Tribunal, en sesión de fecha diecisiete de octubre de dos mil doce.[140]

Ya se ha visto que, en principio de cuentas el Agente del Ministerio Público, imposible que pudiese ordenar, durante la persecución de los delitos e incluso, durante la investigación, la reproducción de los archivos contenidos en los aparatos informáticos, como el caso preciso del celular. Superado ese primer momento, cuando la Suprema Corte de Justicia de la Nación pronuncia, salvo que sea mediante autorización expresa de la autoridad judicial federal y finalmente, como se considera a continuación, se advierte que al asegurar bienes tecnológicos, utilizados en la posible comisión de un delito, por estar abandonados en un lugar donde no hubo detenido, entonces no se viola ninguna garantía fundamental cuando el Ministerio Público ordena extraer la información, como se indica:

DERECHO A LA INVIOLABILIDAD DE LAS COMUNICACIONES PRIVADAS. SI EL MINISTERIO PÚBLICO ORDENA EXTRAER LA INFORMACIÓN CONTENIDA EN UN TELÉFONO CELULAR QUE FUE ASEGURADO POR ESTAR ABANDONADO EN EL LUGAR PROBABLE DE LA COMISIÓN DE UN DELITO Y SIN QUE EXISTA DETENIDO ALGUNO, NO VIOLA DICHA PRERROGATIVA FUNDAMENTAL.

Conforme al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, todas las formas existentes de comunicación y las que son fruto de la evolución tecnológica, deben protegerse por el derecho fundamental a su inviolabilidad. Al respecto, la Primera Sala de la Suprema Corte de Justicia de la Nación en la jurisprudencia 1a./J. 115/2012 (10a.), estableció que ese derecho se extiende a los

[140] Tesis: 1a./J. 115/2012 (10a.) *Semanario Judicial de la Federación y su Gaceta*, Décima Época, t. 1, febrero de 2013, p. 431.

datos almacenados en los teléfonos móviles que son asegurados a las personas detenidas sujetas a investigación por la posible comisión de un delito; aparatos en los que se guarda información privada, ya sea en forma de texto, audio, imagen o video, y de la cual la autoridad investigadora para tener acceso a ella, debe solicitar a un Juez la intervención de la comunicación privada conforme al texto constitucional en cita. Sin embargo, cuando el Ministerio Público ordena extraer la información contenida en un teléfono celular que es asegurado por encontrarse abandonado en el lugar probable de la comisión de un delito y sin que exista detenido alguno, no viola esta prerrogativa fundamental, pues la protección a la información pertenece exclusivamente a la intimidad de la persona titular del derecho protegido, por lo que si en el caso real y concreto no existe algún titular, por no haber detenido con motivo de los hechos o poseedor identificado de éste, es incuestionable que el Ministerio Público, conforme a sus facultades de investigación del delito en términos del artículo 21 constitucional, está facultado para ordenar la extracción de la información almacenada sin que medie la solicitud correspondiente a la autoridad judicial, lo cual no implica violación al derecho fundamental a la inviolabilidad de la comunicación privada y, por ende, que esa información no sea considerada como ilícita, en razón de que las pruebas obtenidas a partir de ésta, no serían esencialmente causa de los datos obtenidos, sino que derivarían de la facultad constitucional de la investigación realizada.

NOVENO TRIBUNAL COLEGIADO EN MATERIA PENAL DEL PRIMER CIRCUITO. AMPARO EN REVISIÓN 244/2012. 7 de febrero de 2012. Mayoría de votos. Disidente: Guadalupe Olga Mejía Sánchez. Ponente: Emma Meza Fonseca. Secretaria: María del Carmen Campos Bedolla.[141]

Finalmente, la Corte ha dejado muy en claro, cual es momento preciso en que un correo electrónico se encuentra interceptado, por tanto al tratarse de una prueba de suma importancia en la determinación de un sinfín de delitos, incluidos aquellos motivo de esta investigación, entonces las autoridades al perseguir e

[141] Tesis: I.9o.P.25 P (10a.) *Semanario Judicial de la Federación y su Gaceta*, Décima Época, t. 3, abril de 2013, p. 2108.

investigar los ciberdelitos, mientras llega el momento legal, deberán observar que *se entenderá que un correo electrónico ha sido interceptado cuando -sin autorización judicial o del titular de la cuenta-, se ha violado el password o clave de seguridad. Es en ese momento, y sin necesidad de analizar el contenido de los correos electrónicos, cuando se consuma la violación al derecho fundamental a la inviolabilidad de las comunicaciones privadas.*

DERECHO A LA INVIOLABILIDAD DE LAS COMUNICACIONES PRIVADAS. MOMENTO EN EL CUAL SE CONSIDERA INTERCEPTADO UN CORREO ELECTRÓNICO.

El correo electrónico se ha asemejado al correo postal, para efectos de su regulación y protección en el ordenamiento jurídico. Sin embargo, es necesario identificar sus peculiaridades a fin de estar en condiciones de determinar cuándo se produce una violación a una comunicación privada entablada por este medio. A los efectos que nos ocupan, el correo electrónico se configura como un sistema de comunicación electrónica virtual, en la que el mensaje en cuestión se envía a un "servidor", que se encarga de "enrutar" o guardar los códigos respectivos, para que el usuario los lea cuando utilice su operador de cuenta o correo. La utilización del correo electrónico se encuentra supeditada a una serie de pasos determinados por cada servidor comercial. Así, es necesario acceder a la página general del servidor en cuestión, donde se radican todos los mensajes de la cuenta de correo contratada por el titular. Esta página suele estar compuesta por dos elementos: el nombre de usuario (dirección de correo electrónico del usuario o login) y la contraseña (password). De vital importancia resulta la contraseña, ya que ésta es la llave personal con la que cuenta el usuario para impedir que terceros puedan identificarla y acceder a la cuenta personal del usuario. La existencia de esa clave personal de seguridad que tiene todo correo electrónico, lo reviste de un contenido privado y por lo tanto investido de todas las garantías derivadas de la protección de las comunicaciones privadas y la intimidad. En esta lógica, se entenderá que un correo electrónico ha sido interceptado cuando -sin autorización judicial o del titular de la cuenta-, se ha violado el password o clave de seguridad. Es en ese momento, y sin necesidad de analizar el contenido de los correos electrónicos, cuando se consuma la violación al derecho fundamental a la inviolabilidad de las comunicaciones privadas. No sobra

señalar, que si bien es cierto que un individuo puede autorizar a otras personas para acceder a su cuenta -a través del otorgamiento de la respectiva clave de seguridad-, dicha autorización es revocable en cualquier momento y no requiere formalidad alguna. Asimismo, salvo prueba en contrario, toda comunicación siempre es privada, salvo que uno de los intervinientes advierta lo contrario, o bien, cuando de las circunstancias que rodean a la comunicación no quepa duda sobre el carácter público de aquélla.

AMPARO DIRECTO EN REVISIÓN 1621/2010. 15 de junio de 2011. Cinco votos. Ponente: Arturo Zaldívar Lelo de Larrea. Secretario: Javier Mijangos y González. [142]

3.4.2. La competencia de las policías para investigar los ciberdelitos en México

Al respecto nos comenta Nava Garcés que en México la Policía Cibernética, a nivel Federal, atiende la parte visible que se muestra en Internet, esto es:

> Revisa, navega, por las páginas en las que se muestran imágenes de pornografía infantil. Luego de detectarlas, busca los enlaces hasta descubrir desde que servidor se generan dichas imágenes. Si este último se encuentra en territorio nacional, entonces lo informa al Ministerio Público de la Federación, para que inicie la averiguación previa[143] correspondiente y con ello se requiera al juzgador para que obsequie la orden de cateo a efectuarse en lugar donde se generan imágenes.[144]

---

[142] Tesis: 1a. CLIX/2011, *Semanario Judicial de la Federación y su Gaceta*, Novena Época, t. XXXIV, agosto de 2011, p. 218.

[143] A partir de la entrada en vigor del proceso penal *acusatorio*, la Averiguación Previa en su nombre y esencia será sustituida por la carpeta de investigación, que es una bitácora del agente del Ministerio Público, para llevar registro de la investigación que realiza que, a diferencia del expediente en la averiguación previa, como regla general, (antes de ser imputada la persona puede tener conocimiento de la investigación e incluso así poder optar por una salida alternativa) deberá hacerla del conocimiento de la defensa a partir de la citación judicial para la formulación de la imputación, y no se hará entrega de la misma al Juez, puesto que se trata de material propio de una de las partes. El nuevo proceso penal implica romper con la existencia de material probatorio que se incorpora automáticamente al proceso por el solo hecho de agregarse al expediente y correspondiente pliego de consignación. Como se explicará en la etapa relativa al juicio oral, todos los medios probatorios deberán ser incorporados por las partes en la audiencia respectiva.

[144] Nava Garcés, Alberto Enrique, *op., cit.*, nota 55, p. 53.

De tal suerte que dicha policía cibernética a nivel federal, desarrolla una Base de Datos Nacional para la identificación de patrones, rangos, preferencias y *modus operandi* de los casos reportados de menores extraviados, desaparecidos, abusados sexualmente, explotados, traficados y prostituidos, además de la integración de un Banco de Datos sobre pedofilia y agresores sexuales.

3.4.2.1. Policías Cibernéticas en las Entidades Federativas

A nivel estatal Jalisco cuenta con una Policía Cibernética que fue creada con la finalidad de detectar por medio del patrullaje en la red, los sitios, procesos y responsables de las diferentes conductas delictivas que se puedan cometer en contra y a través de medios informáticos y electrónicos. En los últimos seis años ha desactivado tres mil 788 sitios relacionados con pornografía infantil. [145]

El Estado de México también cuenta con su propia Policía Cibernética, que tiene como función detectar a los delincuentes que realizan amenazas, cometen fraudes y delitos diversos a través de Internet. Asimismo, la Policía Cibernética atiende cada semana en promedio entre tres y cuatro casos relacionados en su mayoría con secuestros y amenazas. [146]

---

[145] La Fiscalía General del Estado a través de la coordinación de Policía Cibernética brinda orientación a la ciudadanía respecto de los pasos que deberá seguir para presentar una denuncia en caso de ser víctima de un delito cometido a través del uso de las tecnologías de la información, además de que la Policía Cibernética colabora con el Ministerio Publico de así requerirlo en las investigaciones, disponible en: *http://fge.jalisco.gob.mx/policia-cibernetica*

[146] Sistema de Información legislativa, Cámara de Senadores, Periodo 1o Ordinario del II Año de Ejercicio de la LXII Legislatura. 21 de noviembre de 2013. Los suscritos, Senadores MARÍA VERÓNICA MARTÍNEZ ESPINOZA ERNESTO GÁNDARACAMOU, ISMAEL HERNÁNDEZ DERAS, LUIS ARMANDO MELGAR BRAVO, JOSÉASCENCIÓN ORIHUELA BÁRCENAS, GRACIELA ORTIZ GONZÁLEZ y RENÉ JUÁREZCISNEROS, integrantes de la fracción parlamentaria del Partido Revolucionario Institucional, con fundamento en los artículos 71, fracción II, de la Constitución Política de los Estados Unidos Mexicanos; 8, numeral 1, fracción II y 276 del Reglamento del Senado de la República, sometemos a la consideración de esta Honorable Cámara de Senadores, la siguiente proposición con Punto de Acuerdo por el cual se exhortar a todas las entidades del país a fortalecer o en su caso crear sus respectivas policías cibernéticas, como una forma de combatir de manera más efectiva las nuevas modalidades de delitos en México; disponible, *http://sil.gobernacion.gob.mx/Reportes/Sesion/ReporteSesion.php?CveSesion=304264&Origen=BS&Camara=2*

Coahuila a través de su procuraduría estatal tiene su Policía Cibernética que en seis años de existencia ha trabajado con el objetivo de prevenir y perseguir delitos cometidos a través de la red o cualquier aparato que tenga acceso a las redes o que almacene datos.[147] Durante este tiempo se han realizado más de 100 investigaciones, en los que se contemplan delitos como, robo de identidad, fraudes realizados a través de Internet, amenazas, extorsiones, secuestros, entre otros.

En el Distrito Federal, la Policía de Ciberdelicuencia Preventiva fue creada el 3 de abril de 2013, por instrucciones del Secretario de Seguridad Pública, del Distrito Federal, Jesús Rodríguez Almeida, su misión es prevenir la comisión de delitos que usan como medio el Internet, en apego al marco jurídico y respetando los derechos humanos, a través de la generación de productos de inteligencia que permitan elevar la información al grado de certeza. Como principales líneas de acción la Policía de Ciberdelincuencia Preventiva realiza:

> Monitoreo de redes sociales y sitios web en general, pláticas informativas en centros escolares e instituciones del Distrito Federal, con el objetivo de advertir los delitos y peligros que se cometen a través de Internet, así como la forma de prevenirlos, creando una cultura de autocuidado y civismo digital y ciberalertas preventivas las cuales se realizan a través del análisis de los reportes recibidos en las cuentas de la Policía de Ciberdelincuencia Preventiva.[148]

Asimismo, el Estado de Sinaloa cuenta con su Policía Cibernética. De acuerdo con autoridades locales, ello “ante el grave impacto que está teniendo el delito cibernético, que aunque no está tipificado como un delito, todos puede ver cómo el sicópata sexual, el extorsionador y el secuestrador están entrenados por la vía del Internet”.[149]

---

[147] *Idem.*

[148] *http://www.ssp.df.gob.mx/Pages/Ciberdelincuencia.aspx*

[149] *http://sil.gobernacion.gob.mx/Reportes/Sesion/ReporteSesion.php?CveSesion=304264&Origen=BS&Camara=2*

Yucatán también cuenta con la Policía Cibernética de la Fiscalía General del Estado (FGE) respecto a temas como el *ciberbullying, hackeo, crackeo, cibergraffiti* y virus, entre otros temas de actualidad relacionados con el uso que los jóvenes dan a las redes sociales.[150]

Algunos Estados como Hidalgo, Veracruz y Nuevo León, ya han anunciado que están analizando la creación de sus respectivas policías cibernéticas, ello ante la recurrencia de delitos en Internet como son redes de prostitución y pornografía infantil, *hackers,* extorsionadores, fraudes, robo de identidad y otras variantes de expresiones delincuenciales.[151]

3.4.3. Cooperación nacional e internacional entre las policías

La cooperación tanto a nivel nacional como internacional, muchas veces dificulta la investigación de los ciberdelitos. Así lo explica Velasco San Martín:

> Si bien las unidades de investigación policíacas cuentan con facultades para investigar delitos, es el propio Poder Judicial a través de los Ministerios Públicos los que están legitimados para realizar investigaciones judiciales, obtener pruebas y los elementos jurídicos necesarios para encuadrar los tipos penales y poder perseguir delitos. Sin embargo, todavía falta desarrollar vínculos de cooperación bilateral más formales entre el personal de ambas instituciones, puesto que la ausencia de mecanismos de cooperación limita y obstaculiza seriamente las investigaciones y actuaciones procesales en materia penal para procesar debidamente a ciberdelincuentes.[152]

[150] *Idem.*
[151] *Idem.*
[152] Velasco San Martín, Cristos, *op., cit.*, nota 51, p. 368.

3.4.3.1. Jurisdicción

Si el autor de un ilícito se encuentra en un país, el ataque se realizan desde servidores localizados en otra jurisdicción y los efectos se producen en un tercer territorio, resulta evidente que, además de los problemas probatorios anteriormente mencionados, existen cuestiones relativas a fronteras y jurisdicciones.

La investigación de delitos informáticos pone de manifiesto la importancia de la asistencia legal mutua. Sin la apropiada coordinación, existe el riesgo de búsquedas sin autorización de autoridades extranjeras en sistemas de información situados en otro país.

En este sentido, las formas tradicionales de asistencia jurisdiccional han sido diseñadas para obtener datos históricos o incluso en tiempo real involucrando dos jurisdicciones (habitualmente el domicilio del ofensor y el lugar de producción de los efectos).

La criminalidad informática genera un cambio en dicho paradigma en cuanto las comunicaciones pueden trasladarse por tres o más jurisdicciones diferentes, por lo que el proceso de requisitoria se complica exponencialmente, aumentando las opciones de que los datos se pierdan o se encuentren indisponibles.[153]

Otra problemática es la gran diferencia de los sistemas legales para realizar investigaciones y enjuiciar a delincuentes cibernéticos, particularmente cuando existen delitos en donde el delincuente se encuentra en un país distinto en donde el crimen surtió sus efectos o donde las víctimas se encuentren ubicadas. Si bien, existen esfuerzos y mecanismos jurídicos de cooperación bilateral y multilateral como los que se analizaron anteriormente, su implementación requiere de

[153] Iglesias, Gonzalo, *op.,* cit., nota 136, p. 16.

mecanismos más ágiles y flexibles para lograr la cooperación inmediata y poder investigar, detener y procesar a los presuntos delincuentes.[154]

[154] Velasco San Martín, Cristos, *op., cit.*, nota 51, p. 368.

CAPÍTULO 4. LA INVESTIGACIÓN DE LOS CIBERDELITOS: ESPAÑA

4.1. Breve análisis ante la investigación de los ciberdelitos

En España el tratamiento dado a los ciberdelitos, comienza por ser abordado en el nuevo Código Penal de 1995, aprobado por Ley Orgánica de 10/1995, de 23 de noviembre y publicado en el Boletín Oficial del Estado (BOE), número 281, de 24 de noviembre de 1995. Cuyo análisis se llevará a cabo más adelante. No obstante lo anterior, como lo comenta el autor, Santiago Alcurio del Pino, es menester mencionar que:

> Dicho Código Penal incorporó a los tipos delictivos clásicos a la realidad informática de manera global, no limitándose a regular solo los delitos informáticos de mayor conocimiento en la doctrina y otras legislaciones, con ello el legislador intentó lograr la armonía jurídica entre las figuras clásicas penales y el fenómeno informático.[155]

Por ahora no es preciso cuestionar la incorporación de nuevas figuras delictivas a las clásicas, como ya lo hemos mencionado, sino más bien se analizará la manera en que el sistema jurídico se ha adaptado a la inclusión de las nuevas figuras, las que sobra decir, son novedosas por su íntima relación con las nuevas tecnologías.

Por principio de cuentas, es necesario que *la denuncia* o *puesta en conocimiento* se haga ante la autoridad judicial, ministerio fiscal o cuerpo policial que por su función tiene la obligación de perseguir los hechos y sus posibles autores, esos que inicialmente presentan caracteres delictivos.

En innumerables ocasiones la situación se advierte sumamente complicada, debido a que es difícil de comprender y describir y más aun de aportar todos los

[155] Acurio del Pino, Santiago, "Delitos informáticos Generalidades", en: *http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf*

posibles rastros técnicos abandonados por el autor del hecho, son el único camino posible hacia su detección y que, por la naturaleza de los mismos, tienden a desaparecer a una alta velocidad, a medida que va pasando el tiempo desde la comisión, pues son datos que pueden ser alterados o peor aún, eliminados de manera inmediata por sus autores. (Recuérdese que *el autor actúa bajo identidades ficticias, apodos o nicks, suplantaciones de personalidades, entre otros.*)

Por lo tanto, el inicio del éxito en este tipo de investigaciones, a decir de los juristas expertos, será la inmediata denuncia para evitar que los rastros que se hayan dejado se pierdan con el tiempo y con la denuncia deberán acompañarse el mayor número de datos que sea posible, así lo manifiesta Eloy Velasco Núñez:

> El primer rasgo característico necesario en la investigación de este tipo de delitos es el que la denuncia se haga cuanto antes y lo más cerca posible de la comisión de los hechos que se exponen, hechos que deberán ser amparados siempre por el acompañamiento de cuantos más datos sean posibles, esto es por ejemplo, datos técnicos que se tengan como lo son cabeceras de correo electrónico, datos de conexión, señas de página web, etc., de los efectos y rastros dejados por el delito.[156]

La manera en la que se conducen los autores del ciberdelito, la hemos analizado en un capítulo previo, empero, sirva subrayar que las identidades falsas creadas mediante la confianza de saberse protegidos por un ordenador o bien por cualquier otro aparato novedoso que sirva para navegar por los rincones de la red, los llevan a poder reemplazar personalidades, así es mucho más sencillo hacerse pasar por personas inexistentes y permanecer en el anonimato y aún mejor les resulta poder llevar a cabo sus actividades delictivas aprovechándose de los beneficios que les brinda, por ejemplo, el hecho de traspasar las barreras de la territorialidad, el idioma, las clases sociales, así entonces su entorno se vuelve perfecto.

,

[156] Velasco Núñez, Eloy, *op, cit.,* nota 119, p. 77

Ahora bien, en la medida que avanza el uso de la tecnología, cada vez es más compleja la investigación de estos delitos; empero, no imposible, dado que a la par de estos ilícitos han surgido nuevas tecnologías que hacen que la persecución de estas conductas socialmente reprochables, se vean sino rebasadas, cuando menos, no tan limitadas. Cabe entonces analizar en España, las condiciones en las que las autoridades tendrán que trabajar para incursionar en el mundo del ciberdelincuente, lo que inicialmente nos lleva enfrentar la ausencia de legislación relativa al tema y encontramos que, en España tal como en México, no ha sido la excepción.

4.2. Análisis a la legislación española en materia de ciberdelitos

En un principio y contrario a lo que se pudiese pensar acerca de la legislación española en materia de delincuencia cibernética, halla un rezago de consideración, no obstante haber ratificado España en el año 2010 el Convenio del Consejo de Europa sobre el Cibercrimen y en el que recapitulando, en su artículo 35, señala que para poder adherirse a dicho convenio, los países tendrán, entre otras obligaciones, la de reformar sus leyes penales para incluir a estos delitos.

Aduce al respecto sobre su país el autor español Juan Carlos Ortiz Pradillo que: “Muchos de los países de nuestro entorno más próximo han reformado expresamente su legislación procesal con el objetivo de atajar los nuevos problemas que plantea la delincuencia informática, y han aprovechado para regular nuevas medidas tecnológicas de investigación”.[157]

No es posible dejar de señalar que España ha tenido algunas reformas legislativas asertivas, tanto de manera sustantiva como adjetiva respecto a la regulación y tratamiento de los delitos que deriven de actos relativos al uso de los medios tecnológicos, encontrando las leyes LO 2/2002, de 6 de mayo, 32/2003, de

[157] Ortiz Pradillo, Juan Carlos, *Problemas procesales de la Ciberdelincuencia*, Madrid, Ed. Colex, 2013, p. 168.

3 de noviembre, y 25/2007, de 18 de octubre, la primera reguladora del control judicial previo del Centro Nacional de Inteligencia, la segunda Ley General de Telecomunicaciones (LGT) y finalmente la de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones; así como el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, aprobado por Real Decreto 424/2005, de 15 de abril. [158]

Pese a lo anterior, no es suficiente para los españoles, ya que, verbigracia, desde 1988 hubo lugar a una reforma de la Ley de Enjuiciamiento Criminal (LECrim) en cuyo artículo 579, se hacía una inclusión que permitía el uso de las intervenciones telefónicas, artículo que hoy a más de veinte años, sigue siendo el utilizado para la regulación de las novedosas medidas tecnológicas de investigación, de tal suerte que es urgente la aprobación de una Ley que regule de manera precisa y detallada un sistema que facilite la investigación de los delitos cometidos mediante la utilización de las modernas formas de interconexión por satélite, ondas etcétera.

4.2.1. Análisis al Código Penal español de 1995

En su análisis del nuevo Código Penal español, Laura Zúñiga Rodríguez, ha señalado:

> Con anterioridad a la aprobación del nuevo Código Penal (CP) de 1995, la legislación española no contemplaba vías certeras de incriminación de lo que denominamos *conductas de criminalidad informática.* El anterior Código Penal que en su estructura básica provenía de los Códigos Penales del siglo XIX, pese a las múltiples reformas a que había sido sometido, no ofrecía rendimiento interpretativo para el castigo de la delincuencia informática tanto en el ámbito de los delitos

[158] Cabe hacer mención, que la autora de este trabajo realicé un estancia corta de investigación en la Universidad Autónoma de Madrid, España, lo que me permitió durante casi tres meses, poder tener acceso a la inmensa cantidad de fuentes bibliográficas que existen en la biblioteca de dicha Universidad, por tanto el párrafo que se cita es producto de la labor investigativa que llevé a cabo.

patrimoniales (por ejemplo, estafa), como el ámbito de los delitos contra los bienes jurídicos de la persona (por ejemplo, delitos contra la intimidad). El nuevo texto legal de 1995 ofrece un conjunto de previsiones legales que permiten la incriminación de conductas de abuso informático en diversos ámbitos de protección de bienes jurídicos.

En el ámbito de los delitos contra la intimidad, el legislador penal de 1995 efectúa una apuesta decidida por la represión de los delitos informáticos. En este ámbito la decisión político-criminal vino precedida de una ley de protección de datos personales automatizados en 1992 (LORTAD, 1992). Esta Ley Orgánica de desarrollo constitucional, que contemplaba infracciones administrativas, ya anticipaba en su exposición de motivos que el nuevo Código Penal iba a contemplar delitos contra la intimidad cometidos mediante el uso ilícito de la informática.

En otros ámbitos, la opción por crear delitos informáticos se impuso ante la imposibilidad de castigar la criminalidad informática a través de las tradicionales figuras delictivas en el ámbito de los delitos, contra el patrimonio (estafas y delitos de daños). En este sentido la expansión de la informática y la correspondiente fenomenología criminal en este ámbito, así como la evolución del derecho comparado han sido factores decisivos para que el Código Penal de 1995 optase por contemplar delitos informáticos.[159]

Es de suma importancia hacer mención, que en este nuevo Código Penal de 1995 no se creó un Título específico referente a la criminalidad informática, o una legislación especial, como se había hecho en otros países, sino que se optó por una vía intermedia. Así pues, frente al modelo legislativo anterior, en el que no se contemplaba la informática ni como medio de comisión de delitos ni como objeto de protección, en el Código de 1995 se toma en consideración, de forma específica, la informática en relación con diversas modalidades delictivas.[160]

[159] Zúñiga Rodríguez, Laura, *et al. Derecho Penal, Sociedad y Nuevas Tecnologías,* Salamanca, España, Ed. Colex, 2001, p. 111.

[160] Corcoy Bidasolo, Mirentxu, "Problemática de la Persecución Penal de los denominados delitos Informáticos: Particular referencia a la participación criminal y al ámbito espacio temporal de comisión de los hechos", revista EGUZKILORE, número 21, año 2007, p. 31.

Primeramente, tenemos en los delitos contra la intimidad, de descubrimiento y revelación de secretos, en los delitos contra la indemnidad y libertad sexual, de corrupción de menores, en los delitos contra la propiedad, como la estafa, o en los delitos contra el mercado y los consumidores, el acceso a servicios de radio, televisión o servicios interactivos prestados por vía electrónica, en todos ellos se utiliza la informática como medio de comisión de delitos.[161]

Asimismo, la informática –*Hardware* y *Software*–, como objeto de protección se toma en consideración en los delitos contra la propiedad intelectual, protegiendo, en particular, los programas y en los delitos de daños –daños o *sabotaje* informático.[162]

A ello hay que sumar otras conductas delictivas, realizadas a través de Internet, que pueden castigarse sin necesidad de crear tipos específicos, así, por ejemplo, delitos contra la libertad, como amenazas y coacciones, delitos contra el honor, falsedades, defraudación de telecomunicaciones, revelación de secretos de empresa –espionaje industrial–, delitos contra la propiedad industrial, publicidad engañosa, blanqueo de capitales.[163]

Como se observa, la generalidad de las aportaciones de los juristas se encuentran en concordancia, lo que es indiscutible es que este Código incorporó las conductas delictivas de ciberdelincuencia a sus figuras antiguas para poder perseguir, investigar y sancionarlos.

De tal suerte que Fermín Morales Prats Catedrático de Derecho Penal Universidad Autónoma de Barcelona, asume la postura relativa a los delitos informáticos señalando la viabilidad al no optarse por crear un título autónoma, sino que conlleva la misma apreciación, esto es que:

---

[161] *Idem*
[162] *Idem*
[163] *Ibídem,* p. 32.

> De manera trasversal- en cuanto a los diversos bienes jurídicos afectados-pasase a contemplar las diversas conductas típicas en atención a la insidiosidad de los medios técnicos utilizados. Sin embargo, se ha optado por una decisión político-criminal, a juicio a su parecer ha sido loable, que las infracciones se encuentren distribuidas a lo largo del Código Penal en diversos títulos, que atienden a las necesidades diversas de protección que en cada caso se identifican para bienes jurídicos de naturaleza también diversa (intimidad, patrimonio, secretos de empresa.)[164]

Por otra parte Carmen Adán del Río, Fiscal del Tribunal Superior de Justicia del País Vasco, menciona que cierto es que, la utilización de los tipos penales tradicionales para supuestos de hecho relacionados con la informática tiene sentido en ocasiones, su incorporación o no, a las figuras tradiciones, en algunos casos puede o no, ser loable y es que, esto es a decir del Fiscal porque, se puede cubrir con referencias como la del artículo 26 del Código Penal, que nos habla acerca del documento informático (*todo soporte material que exprese o incorpore datos o hechos con eficacia probatoria o relevancia jurídica, da plena vigencia penal al documento informático),* lo que permite, en el caso preciso, durante la investigación, aplicar toda la doctrina sobre las falsedades a los casos de falseamiento de documentos y registros informáticos. Afirmando: "De hecho, en nuestro trabajo diario, vemos alegaciones o pronunciamientos que intentan convertir los artículos dedicados a las falsedades en un tipo al que recurrir, cuando muchos de esos casos no puedan reconducirse a los tipos específicamente informáticos."[165] Determinando así que en la cotidianidad se pueden encuadrar conductas delictivas relativas a las nuevas tecnologías, es decir la ciberdelincuencia, a los tipos penales tradicionales.

4.2.2. Principios de Legalidad

[164] Zúñiga Rodríguez, Laura, *op., cit.,* nota 159 p. 12

[165] Adán del Río, Carmen*, La persecución y sanción de los delitos informáticos*, revista EGUZKILORE, número 20, diciembre de 2007, pp. 151-161

Sin importar el obsoletísimo y lo raquítica que pueda ser la legislación procesal española, los tribunales han admitido –y en su caso, condicionado- el uso de los avances tecnológicos, en las labores de la investigación criminal, concientes de que la inexistencia de una normativa expresa que regule la posibilidad de utilizar los nuevos avances tecnológicos supone acrecentar las desventajas con las que se encuentran las fuerzas y cuerpos de seguridad a la hora de proceder a la indagación y descubrimiento de los instrumentos y pruebas delitos. Sabedores de que de ser así se dejaría un amplio campo de acción a la ciberdelincuencia. [166]

Por tanto, los Tribunales y especialmente el Tribunal Supremo, han legitimado el uso de las nuevas tecnologías de investigación, subsanando las importantes lagunas de la legislación española, mediante el proceso de jurisprudencia.

El ejemplo que cabe citar es el relativo a la intervención de las telecomunicaciones, en el que pese a la regulación insuficiente y obsoleta que se contempla en el artículo 579 de la LECrim, ha sido cubierta la laguna legal presentada en dicho precepto de manera jurisprudencial respaldada por el Tribunal Europeo de Derechos Humanos (TEDH), ocupándose el Tribunal Supremo de ampliar la interpretación para dar lugar a regular así también la intervención a los correos electrónicos o bien otras actividades realizadas mediante la red. [167]

Es cuestionable entonces, si no hay una legislación que regule la interceptación de las comunicaciones, cuan valido podrá ser el hecho de que únicamente a través de la jurisprudencia se puedan subsanar las lagunas legales que protejan la actuación de las autoridades competentes en la investigación de los delitos cometidos en la era digital; dado que se puede presentar como un arma de doble filo, ya que aun cuando no está debidamente regulado, siempre que los órganos jurisdiccionales, hayan actuado respetando las exigencias del principio de

[166] Ortiz Pradillo, Juan Carlos, *op., cit.,* nota 157, p. 171.
[167] *Idem.*

proporcionalidad un acto ilegítimamente constitucional queda justificado dando pauta a que en el cumplimiento se cometan excesos e incluso se vulneren los derechos de los investigados o cualquier ciudadano.

4.2.3. Jurisdicción y Competencia

A fin de analizar la jurisdicción tocante cuando se comete un ciberdelito, en el territorio español obsérvese la manera de abordarlo de la Catedrática de la Universidad de Barcelona Mirentxu Corcoy Bidasolo, quien indica que:

> El lugar de comisión de hechos ilícitos cometidos a través de la informática suscita problemas similares a los relativos al momento de comisión del delito y la delimitación entre los concursos de leyes y de delitos. Para la criminalidad cibernética, especialmente si se comete a través de Internet, la legislación penal concebida tradicionalmente como cuerpo legislativo vigente para un determinado territorio no es válida. No obstante, es cierto que el problema no es exclusivo de la criminalidad informática sino que es una de las consecuencias de la criminalidad transnacional. Aunque finalmente ésta también es posible por la utilización de las nuevas tecnologías. Al respecto hay dos soluciones, que pueden ser concurrentes: a) armonización de las legislaciones y facilitamiento de los mecanismos de cooperación internacional; b) establecer cláusulas de extraterritorialidad, tal y como ya existen en materia de terrorismo, genocidio, tráfico de personas.
>
> En el supuesto de la criminalidad informática, en el Código Penal se ha previsto la extraterritorialidad en la corrupción de menores, artículo189 1. b), donde se castiga: "la producción, venta, difusión o exhibición por cualquier medio de material pornográfico en cuya elaboración hubiesen sido utilizados menores de edad o incapaces, o lo poseyere para estos fines, a aunque el material tuviere su origen en el extranjero o fuere desconocido." [168]

[168] Corcoy Bidasolo, Mirentxu, *op., cit.,* nota 160, p. 31

Las mayores dificultades en el ordenamiento jurídico español para determinar el órgano judicial competente para el enjuiciamiento de delitos cometidos a través de Internet se plantea desde dos perspectivas.

En primer lugar respecto a la determinación de la competencia objetiva, la dificultad reside en determinar, por razón de la materia, en que supuestos el delito deber ser investigado por los juzgados de instrucción (y posteriormente enjuiciado por el órgano competente en función del tipo de delito o de la gravedad de la pena que lleve aparejada) y cuando ha de ser objeto de investigación por los Juzgados Centrales de Instrucción de la Audiencia Nacional, porque se trate de uno de los supuesto establecidos en el artículo 65 Ley Orgánica LOPJ.[169]

En segundo plano, y respecto a la determinación de la competencia territorial, el problema se centra en determinar en qué lugar se entiende cometido el delito, a los efectos establecidos en los artículos 14.2 y 15 LECrim, ya que, precisamente por tratarse de delitos a distancia, el lugar desde donde actúa el autor y pone en marcha su plan delictivo puede encontrarse a cientos o miles de kilómetros del lugar donde tales actos producen sus perniciosos efectos.[170]

Indica el autor Juan Carlos Ortíz Pradillo que de acuerdo con el listado establecido en artículo 65 LOPJ, es posible colegir que los ciberdelitos que deberían ser enjuiciados ante la Audiencia Nacional pueden ser agrupados en las siguientes categorías:

> Primer categoría los delitos establecidos en los capítulos II y III del Título XXI del Libro II del Código Penal, refiérase entonces a los delitos contra la Corona y a los delitos contra las Instituciones del Estado y división de poderes, respectivamente, en donde es incuestionable a razón de que varios de ellos pueden ser cometidos a través de Internet. A manera de ejemplo tenemos que en el delito previsto en el artículo 491 del Código Penal, se han dictado varias condenas por parte de la

[169] *Crf.* Ortiz Pradillo, Juan Carlos, *op., cit.,* nota 157, p. 45
[170] *Idem.*

Audiencia Nacional, basándose en dicho precepto pues ha sido violado al publicar injurias y calumnias contra la Corona difundidas a través de prensa, radio y televisión, así que, teniendo en cuenta la competencia de la Audiencia Nacional para estos casos no hay motivo alguno que pueda impedir que los actos que violenten el precepto legal en comento, mediante la utilización de Internet como medio de difusión, no puedan ser competencia de la dicho Órgano Judicial. Asimismo tenemos dentro de sus facultades competentes lo dispuesto por el artículo 494 del citado ordenamiento, relativo a la promoción a través de Internet de manifestaciones, o cualquier clase de reuniones ante las sedes del Congreso de los Diputados, del Senado o de una Asamblea Legislativa de Comunidad Autónoma, cuando estén reunidos alterando su normal funcionamiento.

Como segunda categoría podemos ubicar el ciberterrorismo y las actividades relacionadas con el terrorismo, corresponde entonces observar lo establecido en el artículo65.7° LOPJ, y de la Disposición Transitoria de la LO 4/1998, que indica que es competencia de la Audiencia Nacional conocer de los delitos de terrorismo y dado que el terrorismo estrechamente se encuentra vinculado a la era de las tecnologías, para su preparación, difusión y ejecución, podemos analizarlo por una parte como aquella actividad que pone en riesgo y vulnera la estabilidad en la infraestructura de los Estados atacando a sus propios sistemas a través de la Red, es decir el ciberterrorismo y por otro lado todas aquellas conductas terroristas que echan mano del uso de las tecnologías e Internet, como herramientas para lograr la comisión de los delitos, desde comunicación entre sus miembros, difusión mediante Internet de propaganda y actos grabados en los que se muestra cómo fabricar y utilizar explosivos e incluso invitaciones al reclutamiento de activistas.

Finalmente como tercera categoría tenemos que es competencia de la Audiencia Nacional conocer de los delitos de falsificación, siempre que sean realizadas o fabricadas por una organización o grupo criminal, y que consistan en la duplicidad de tarjetas bancarias cuyos números sean obtenidos fraudulentamente, así como la fabricación de cheques de viaje falsos y la falsificación de moneda. Esta actividad se logrará cuando la organización criminal utilice para la fabricación el empleo de

programas informáticos especializados o bien la numeración, que previamente le corresponda a un cliente, la llamada *clonación.* [171]

4.2. Autoridades españolas investigadoras del ciberdelito

La complejidad de la acción delictiva y la necesidad de ciertos conocimientos técnicos para iniciar el rastreo del delito en busca de su autor, conllevan a la necesidad de una cierta especialización en quienes investigan estos delitos, desde los cuerpos policiales que recogen la denuncia e inician los seguimientos técnicos sobre los vestigios delictivos, hasta el fiscal o juez que deben decidir sobre su continuación. [172]

De ahí que la Policía y la Guardia Civil mediante sus respectivas Brigadas de Investigación Tecnológica y grupo de delitos telemáticos hayan creado sus correspondientes secciones "especializadas en la investigación de este tipo de delitos (tanto transversal como directamente) y convenientemente las hayan territorializado por todo el territorio de la nación, de manera similar a lo que después ha realizado el ministerio fiscal".[173]

Dado lo anterior y como mero antecedente en 1996, la Guardia Civil, crea el grupo de Delitos Informáticos, que posteriormente en 1999 cambiará su denominación a grupo de Delitos de alta Tecnología, cuya constante evolución lleva a que en el año 2000, dicho sea de paso, previo a la firma del Convenio del Consejo de Europa sobre el Cibercrimen o Convenio de Budapest, se origine el Departamento de Delitos Telemáticos, dentro del que se ubica el actual Grupo de Delitos Telemáticos.

Que dentro de las principales funciones de este grupo cabe destacar el desarrollo de investigaciones relacionadas con la delincuencia informática,

---

[171] *Idem.*
[172] Velasco Núñez, Eloy, *op, cit.,* nota 119, p. 69.
[173] *Ibidem,* p. 70.

representar y promover la participación de la Guardia Civil en foros y encuentros internacionales sobre cibercrimen, así como establecer un punto de contacto de cooperación internacional en el ámbito de cibercrimen.

4.2.1. Perfil del policía cibernético en España

Siguiendo con ese orden de ideas, es menester que quienes conforman el grupo de delitos telemáticos cuenten con conocimientos suficientes en informática, técnica procesal penal, experiencia investigadora, relaciones internacionales y cuyo profesionalismo sea cuestionable en ningún momento, dado que la investigación, como todas, empero, tratándose de situaciones complejas, que incluso pueden vulnerar la seguridad de un Estado, como lo es los ataques cibernéticos, se requiere de la absoluta discreción del investigador.

4.3.2. Diligencias de investigación

Ahora bien, para asegurar el éxito de una investigación, existe dentro del proceso una variada gama de diligencias que pueden ser practicadas, sin embargo la mayor parte del tiempo, los encargados de hacer dichas diligencias, se encuentran con diversas problemáticas que dilatan los resultados, máxime cuando de no vulnerar Derechos Fundamentales, se trata, debido a que esta consigna es Universal, en España como cualquier país del mundo, deberán observarse los más amplios criterios que eviten la violación por parte de las autoridades a los particulares, obsérvese pues que dentro de la investigación se halla un elemento subjetivo y uno de los objetivos principales de la instrucción judicial, lo constituye la averiguación de los autores de los hechos investigados, que es, como ya se ha comentado, la situación más difícil de descubrir.[174]

Por tal motivo es de suma importancia que en las diligencias de carácter penal que sean practicadas para lograr el descubrimiento de la identidad de los

[174] Velasco Núñez, Eloy, *op, cit.,* nota 119, p. 77

autores del ciberdelito cometido, los agentes policiales comisionados por el juez no olviden consignar, además de los datos a que se refiere el artículo 569 LECrim, cuantos datos permitan identificar al presumible usuario donde se ocupen los efectos delictivos tales como:

> Archivos y documentos objeto de la investigación, aprehensión de las claves de usuario y contraseña que se descubran, apodos o nicks que se encuentren junto al ordenador, que no se omitan los "pantallazos", incluso imprimiéndolos, y que se consigne la ocupación en su caso de discos duros y otros dispositivos almacenadores de memoria con determinación de su ubicación, y en caso de apertura *in situ* de archivos, directorios o carpetas, que no se escatimen en datos técnicos como serían, por ejemplo, en los supuestos de pornografía infantil, la indicación del número y nombre de los archivos, el número de fotografía infantil, la indicación del número y nombre de los archivos, el número de fotografías e imágenes encontrados, su impresión en soporte duradero y los megas de su capacidad y ocupación.[175]

4.3.2.1. La prueba electrónica

A manera de introducción únicamente, toda vez que el tema fue abordado en un capítulo anterior relativo a la *prueba electrónica* dentro del sistema mexicano. Diremos que en todos los delitos que son cometidos mediante el uso de la tecnología, incluidos obviamente los ciberdelitos, son susceptibles, las evidencias, de ser destruidas o manipuladas, de tal suerte que la obtención de lo que se denomina "prueba electrónica" es sumamente indispensable para demostrar la culpabilidad de un sospechoso.

"La capacidad policial de utilizar cualesquiera medidas tecnológicas de investigación destinadas a obtener esa información en formato digital se antoja un pilar esencial en cualquier investigación criminal, porque podrán ser empleadas en

[175] *Ibidem,* p. 82

cualquier investigación criminal. Resultando que la tecnología puede facilitar las labores policiales de seguimiento e investigación."[176]

La generalización en el uso de la prueba electrónica o prueba por soportes informáticos ante los tribunales presenta, sin embargo, una importante contrapartida a tener en consideración: las expectativas de contar con una prueba inculpatoria, directa de tipo digital que demuestre la comisión del delito, de modo que, a falta de una prueba científica, surjan dudas sobre la autoría de los hechos. Esto es, a medida que se fabrican y emplean nuevos instrumentos y métodos capaces de demostrar científicamente la producción de un hecho, su autor y sus consecuencias, puede llegar a generarse en el juzgador la expectativa de que siempre existirá una prueba científica o electrónica que demuestre el relato de la acusación.[177]

En este campo el jurista Eloy Velasco Núñez manifiesta que es importante y liberador para los investigadores el hecho de saber que cuentan con tecnología que les permitirá probar la historia delincuencial que ha causado un daño socialmente:

> El desarrollo tecnológico ha permitido que las autoridades responsables de la investigación criminal tengan a su disposición nuevos y sofisticados instrumentos electrónicos y programas informáticos capaces de conseguir la interceptación y la grabación en tiempo real de todos aquellos datos transmitidos o recibidos a través de los distintos medios de comunicación (esto es, no sólo el contenido propiamente dicho de las comunicaciones, sino también aquellos datos externos a la comunicación y que ésta lleva aparejados, como por ejemplo los datos de tráfico o los datos de localización) así como también resultan capaces de conseguir acceder a aquellos datos que se encuentren almacenados en las unidades de memoria de los diversos equipos electrónicos o informáticos, lo cual aproxima tales actuaciones policiales al denominado *hacking* o instruismo informático.

[176] *Ibidem,* p. 159.
[177] *Ibidem,* p. 162.

> El empleo de la tecnología en la averiguación de los delitos y la determinación de sus responsables no es simplemente una opción a barajar. Constituye una necesidad en la investigación de determinados delitos, principalmente en aquellos en los que se emplean nuevas tecnologías –ciberdelincuencia-.[178]

Ahora bien, la obtención de la evidencia digital resulta un reto para cualquier legislación en la materia pues, como se ha mencionado, países varios, son los que se encuentran en este proceso. De tal suerte que para la policía resulta un trabajo esencial y en conjunto con peritos expertos en la materia deben realizar un correcto embalaje de la prueba. Cabe aclarar que cualquier rastreo o recuperación de la prueba debe realizarse con el consentimiento de la autoridad de lo contrario se estaría manipulando, lo que conlleva a la violación de la cadena de custodia.

Así entonces la licitud de la prueba electrónica es el primer requisito indispensable y que debe observar el juzgador. En la historia de España específicamente causó controversia un caso en particular, el de la obtención de grabaciones entre abogado y defenso del denominado *caso Gürtel y el Sitel*.

El caso *Gürtel* es el nombre con el que se conoce una investigación iniciada en noviembre de 2007 por la Fiscalía Anticorrupción y denunciada por la Fiscalía en febrero de 2009 ante la Audiencia Nacional, sobre una red de corrupción política vinculada al Partido Popular (PP), que operaba principalmente en las Comunidades de Madrid y Valencia. La trama estaba encabezada por el empresario Francisco Correa Sánchez, cuyo apellido Correa en alemán dio nombre al caso. Se abrió el caso Gürtel tras la denuncia realizada desde Majadahonda por el exconcejal José Luis Peñas, entre otros. Anexo 4

4.3.3. Técnicas de investigación penal vinculadas a las nuevas tecnologías en España

[178] *Ibidem,* pp. 160-163

Para combatir los delitos informáticos complejos, caben diversos métodos complementarios a los convencionales y que a decir Eloy Velasco Núñez, se pueden clasificar de la siguiente manera:

> Intrusivos (infiltración en la Red criminal a través de agentes encubiertos, obtención de información a través de la interceptación de las comunicaciones con el uso de programas espía – v.gr., *e-blasters* y otros monitorizadores a distancia como los teclados *keylogger* -, intervención de ADSL, introducción de "troyanos" espía, o métodos de grabación y/o filmación de actividades);
>
> Coercitivos (entradas y registros, detenciones, comiso de ordenadores);
>
> Disuasorios (uso de delatores y confidentes para los ataques informáticos realizados en grupo organizado);
>
> Cooperacionistas (la figura del "enlace" con las empresas telefónicas, proveedoras de acceso y prestadoras de servicio de Internet);
>
> Preventivos (campañas informativas, medidas de restricción del Uso de Internet, auto judicial de alejamiento informático.) e incluso
>
> Legislativos (que específicamente regulen los métodos intrusivos y en concreto la intervención y registro de comunicaciones telemáticas).[179]

4.3.3.1. Monitorización a distancia

La Monitorización a distancia es una técnica novedosa de investigación penal, utilizada en España, a saber:

> En términos generales se puede llamar monitorización, o el uso de programas informáticos (*software*) capaces de duplicar la información telecomunicativa y el contenido de los archivos de un terminal en otro (el del investigador público con

[179] *Ibidem,* p. 202.

autorización judicial) con el objeto de obtener tal información para verificar o descartar la hipótesis delictiva en que consista la investigación penal.[180]

Su base legal se encuentra en el artículo 579.3f *in fine* LECrim., que permite el acuerdo judicial en resolución motivada por un plazo de hasta tres meses prorrogable de la observación de las comunicaciones de las que se sirvan las personas sobre las que existan indicios de responsabilidad criminal para la realización de sus fines delictivos.

4.3.3.2. Teclados *keylogger*

Sin duda no puede dejar de lado otra técnica novedosa de obtención de información en la materia también se encuentra:

> El *key/logger* (lector de teclados), que ante la necesidad de captar actuaciones interactivas no monitorizables en el investigado (especialmente su clave y su contraseña), pudiera instalarse con autorización judicial como complemento técnico de la que jurídicamente es la interpretación de la información de interés para la investigación en los ordenadores.[181]

4.3.3.3. Infiltración y agente encubierto en Internet

Ahora bien, según lo estipulado en el artículo 282 bis LECrim, hallamos que cuando se trate de investigaciones que afecten a actividades propias de la delincuencia organizada, el juez de instrucción competente y el ministerio fiscal dando cuenta inmediata al juez, *podrán autorizar a funcionarios de la policía judicial*, mediante resolución fundada y teniendo en cuenta su necesidad a los fines de la investigación, *a actuar bajo identidad supuesta* y a adquirir y transportar los objetos, efectos e instrumentos del delito y diferir la incautación de los mismos.[182]

---

[180] *Idem.*
[181] *Idem*.
[182] *Ibidem,* p. 206.

Respecto de la naturaleza del agente encubierto en Internet, se debe propugnar exclusivamente la de extracto policial, de modo que, como ya se ha señalado algunos resoluciones del Tribunal Superior, la ayuda a los cuerpos policiales a infiltrarse y la información/colaboración que aporten denunciantes, testigos protegidos o incluso imputados colaboradores con la justicia, no les convierte en lo que no son, no siendo a tal colaboración aplicable la normativa del artículo 282 bis LECrim.[183] Esto es que el agente encubierto estará actuando estrictamente bajo la legalidad que ponerse la camiseta le da, así tenemos que quedan exentos de ser acusados de la comisión de un ilícito.

A diferencia de lo que ocurre en el mundo convencional, en el virtual, la actuación por agente encubierto, lo normal es que la infiltración sólo pueda realizarse con autorización judicial. De no hacerse de esa manera se corre el riesgo de que las pruebas que se obtengan podrían tener el efecto de no admisibles por la dudosa obtención.

La infiltración extralegal del agente policial encubierto, por su cuenta y sin permiso del juez o fiscal, en que la oficialidad y el privilegio probatorio que supone la judicialización que dota la cobertura el proceso marcada por el artículo 282 bis LECrim., desaparecen, aflorando, además de una “presunción de corrupción policial”. A fin de evitar cualquiera de estas situaciones, siempre es mejor actuar bajo la legalidad que los ordenamientos permiten.

4.3.3.4. Incorporación de las nuevas tecnologías a la Policía española

Es preciso manifestar que desde el punto de vista social, la opinión de la incorporación de las nuevas tecnologías a la policía tiene distintas aceptaciones, máxime cuando se trata de situaciones intrínsecas que tienden un impacto directo

[183] *Ibidem,* p. 208.

en quienes han elegido servir profesionalmente a la comunidad, ha sido manifestado por el Doctor Jesús Requena Hidalgo atendiendo lo siguiente:

> Concentrados en la policía y en su ejercicio profesional cotidiano, hay que decir que la adopción y el uso efectivo de nuevas tecnologías no ha sido un proceso lineal, ni neutro y, desde algunos puntos de vista, cualquier cosa menos armónico. Las experiencias que se tienen de su adopción y su uso efectivo en el ejercicio profesional cotidiano en la policía permiten, si no dudar de sus enormes potencialidades o mostrar un escepticismo que en modo alguno estaría plenamente justificado, sí plantear algunas cuestiones. En algunos casos, la incorporación de estas tecnologías ha encontrado resistencias y ha creado tensiones en el interior de organizaciones cuyos flujos de información y trabajo debía precisamente mejorar; en otros, ha servido para que afloren ciertas disfunciones entre organizaciones de policía diversas que formalmente se integran en un modelo único. Incluso, hay autores que han llamado la atención sobre cierta pérdida de *savoir-faire* en la práctica policial relacionada con la incorporación de estas tecnologías al trabajo cotidiano.[184]

En definitiva no todo está bien o todo es negativo, cierto es que la sociedad evoluciona y con ella los métodos y prácticas, también es cierto que no siempre son aceptables de manera inmediata, como se ha dicho, algunas veces causan resistencia al tratar de incorporarlas y es justificable mencionar que no todos las servidores están preparados para evolucionar a la par. Empero, podrá estarse a favor o en contra de la inclusión de las nuevas tecnologías, lo que es innegable para todo el mundo es que son una necesidad, en el caso concreto de la policía lo son porque gracias a ello, tendrán una manera medianamente equitativa y proporcional para combatir la ciberdelincuencia.

[184] Requena Hidalgo, Jesús, "De la sociedad disciplinaria a la sociedad de control: la incorporación de nuevas tecnologías a la policía" *Scripta nova, revista electrónica de geografía y ciencias sociales,* España, vol. VIII, núm. 170 (43), 1 de agosto de 2004, pp.

4.4. España ante los ciberataques de contenido

Los ciberataques de contenido, según el autor español Fernando Miró Llinares:

> Se trata de una categoría del grupo de tipologías de cibercrimanilidad, en la que el centro de la infracción lo constituye el contenido que se comunica o se transmite a través de las redes telemáticas, particularmente de la Red de redes, Internet, generando una novedosa comunicación entre emisor y receptor, debido a que los papeles pueden invertirse de un momento a otro en el ciberespacio, dando lugar a que el emisor se convierta de pronto en receptor y productor de su propio contenido.[185]

Sin olvidar la gran popularidad, que hoy día muestra la red y que incluso invita a ser utilizado por cualquier tipo de personas, lo que ha llevado desde hace tiempo a generar la preocupación por lo que se difunde en Internet. Los contenidos de Internet son *ilícitos* cuando constituyen delito en sí mismos (v. gr., la difusión pornográfica infantil), siendo merecedores de sanción penal.

4.4.1. Pornografía infantil en Internet

Pese a tratarse de un concepto que socialmente parece no tener discusión, en cuanto a la acepción de su significado, no obstante, no es sencilla la definición de la pornografía infantil, tratándose máxime, de un tema tan delicado que por el simple hecho de llevar la palabra infantil nos puede mostrar lo atroz de la finalidad en su reproducción, y a su vez esa compleja construcción de un concepto unánime de este fenómeno viene dada, por la multiplicidad de factores que en él influyen, tanto de tipo cultural como moral, pero sobre todo por lo confuso y altamente inadecuado del propio término, como ha señalado buena parte de la doctrina.

[185] Miró Llinares, Fernando, *op., cit.,* nota 117, p.101

Entonces pareciera que el concepto proporcionado por el Grupo de INTERPOL especializado en crímenes contra niños, es el más acertado, ya que considera a la pornografía infantil como: “Toda forma de representación o promoción de la explotación sexual de los niños, incluidos los materiales escritos y el audio, que se concentren en la conducta sexual o los órganos genitales de los niños”. [186]

El fenómeno de la pornografía infantil, a pesar de no ser propiamente informático, está cada vez vinculado al uso de las nuevas tecnologías, hasta el punto que, en la actualidad, desde una perspectiva criminológica se puede decir que la mayoría de estos comportamientos se perpetran básicamente a través de Internet.

En España y como muestra de lo anteriormente señalado, la Fiscalía General del Estado en la Consulta núm. 3/2006, de 29 de noviembre destaca que la eclosión de Internet ha revolucionado por completo el mercado de la pornografía infantil hasta prácticamente monopolizarlo, como consecuencia de las ventajas que proporciona a los usuarios, “*desde la facilidad para descargarse archivos, los menores costes económicos, la aptitud para entablar relación con un enorme número de internautas con la consiguiente facilitación de los intercambios y las grandes posibilidades de permanecer en el anonimato*”.[187]

En la misma tesitura, obsérvese el análisis sobre el modo de llevar a cabo dicha actividad, y es que actualmente se ha convertido en una de las principal fuente de negocios en la red, esto es a través de organizaciones criminales, nacionales e incluso de carácter internacional, cuyos integrantes bien podrían pasar como, delincuentes de cuello blanco y es que único fin es que señala Fernando Miró Llinares que:

[186] *Ibidem,* pp. 106-107.
[187] *Ibidem,* p. 112.

> La obtención de beneficios económicos, que realizan sus actividades a través de asociaciones o empresas encubiertas que operan permanentemente. El objetivo económico de estas organizaciones se satisface al abonar el destinatario una determinada cantidad de dinero como contraprestación a la adquisición del material pornográfico; una vez que se abona esta cantidad, recibirá una clave de acceso a la página en cuestión o recibirá las imágenes requeridas vía correo electrónico o contra reembolso, el producto que haya demandado, normalmente un vídeo.[188]

Ahora bien, como es visible a todas luces, los criminales buscan día a día la innovación de las técnicas de producción e introducción del material en la Red y lo que es mejor para los cibercriminales, estas formas de difusión y tráfico de pornografía infantil pueden ser llevadas a cabo desde el anonimato que proporciona Internet. Así por ejemplo tenemos, las que aduce Laura Zúñiga Rodríguez, son formas muy sofisticadas de enmascarar la fuente pues se hallan al alcance de todos, los llamados "*anonimous remailers,* que no son sino el envío de *e-mails* sin remitente, de modo que el remitente envía un correo electrónico a un servidor que, a su vez, lo reenvía al destinatario final sin que aparezcan los datos del remitente".[189]

El empleo de los denominados *computer bulletin boards* (tablones de anuncios de ordenador) también puede constituir otro mecanismo de intercambio de información entre pedófilos, mediante los cuales es posible mantener conversaciones, o bien existe también la posibilidad de utilizar las llamadas salas de *chat* donde los pedófilos pueden mantener *on line* una actividad bajo un contexto sexual con menores.

Finalmente, los avances tecnológicos también han hecho que sea posible encubrir la participan de los adultos en el material pornográfico, a través de la distorsión de imágenes, o bien cuando se trata de colocar una imagen de un menor

[188] *Idem.*
[189] Zúñiga Rodríguez, Laura, *op., cit.,* nota 159, p. 120.

en el cuerpo de un adulto, lo que se denomina pornografía técnica, empero, dicha conducta también debe ser susceptible de sanción penal.

Dentro de los principales puntos de interés, pese a saber que el material es difundido a través de la red, es lógico preguntarse cuál es la procedencia de los niños y victimas afectados por este fenómeno de la pornografía infantil,

Aduce el autor Fernando Miró Llinares que:

> La procedencia de las víctimas varía dependiendo del medio o vía de difusión del material, teniendo así que la pornografía infantil que se difunde a través de DVD en video-clubs normalmente está protagonizada por menores de zonas del Tercer Mundo y Asia, la que se difunde a través de Internet, lo normal es que su protagonistas sean de nacionalidad tailandesa o de algún país asiático. No obstante la Resolución del Parlamento Europeo A5-0052/2000 a otros organismos, sobre la aplicación de las medidas contra el turismo sexual que afecta a los niños, señala expresamente a los países de la antigua Unión Soviética, como núcleo del problema del turismo sexual y la trata de seres humanos, atribuyéndolo a las difíciles condiciones de vida y la fronterización existente con la Unión Europea.[190]

[190] Miró Llinares, Fernando, *op., cit.,* nota 117, pp. 112-113.

CONCLUSIONES

PRIMERA.- La policía, en términos generales, es una institución de servicio público cuyo propósito es satisfacer las necesidades de la comunidad en cuanto a su custodia y seguridad, pero sobre todo, por medio de un servicio de investigación de eficacia y eficiencia.

SEGUNDA.- Después de la lucha armada originada por la Revolución Mexicana, ya en el México moderno la figura de la policía por primera vez tiene un fundamento constitucional, un fundamento que prevalece al día de hoy y en el que se faculta a la policía como órgano investigador, en virtud de que previamente solo se basaba en ordenanzas y reglamentos. (Artículo 21 constitucional)

TERCERA.- En México, desde el año 2000, existe una *policía cibernética* adscrita a la hoy denominada Comisión Nacional de Seguridad Pública, y sus actividades principales consisten en patrullar Internet para rastrear conductas ilícitas, portales, comunidades y *chat romos* en los que se promueven la pornografía y el turismo sexual infantil, entre otros, en territorio nacional. Coahuila**,** el Distrito Federal, Estado de México, Jalisco, Sinaloa y Yucatán cuentan, aun sin legislación que las regule, con su propia policía cibernética y solo las entidades federativas de Hidalgo, Veracruz y Nuevo León, ya han anunciado que están analizando la creación de sus respectivas policías cibernéticas.

CUARTA.- Resulta sumamente complicado determinar cuál es la denominación correcta para las conductas cometidas mediante el uso de la informática, en algunos países se utiliza la expresión *delitos informáticos*, en otros se habla de *ciberdelitos o cibercrimen* o simple y llanamente delitos cometidos a través de sistemas de cómputo e Internet *(computer crime)*. Y para muchos también son nombrados *delitos cibernéticos*. No hay una definición unánime, todas las existentes se hicieron tomando en cuenta diferentes criterios, dependiendo de las perspectivas y

experiencias tanto de quiénes investigan este delito, como de quiénes han sido víctimas del mismo.

QUINTA.- El comité Europeo sobre Problemas de Delincuencia, decidió en 1996 establecer un comité de expertos para tratar aspectos relacionados con el cibercrimen. Se crea entonces el proyecto de Convención sobre Cibercrimen del Consejo de Europa en junio de 2001, dicho Convenio sobre Ciberdelincuencia del Consejo de Europa tiene como objetivos, entre otros, armonizar los elementos sustantivos de la legislación penal relacionada con disposiciones de cibercrimen; ofrecer las facultades necesarias sobre derecho procedimental doméstico para la investigación y persecución de delitos y otras conductas cometidas a través de sistemas de cómputo y para la obtención de pruebas en relación a la información contenida en forma electrónica y establecer un régimen ágil y efectivo de cooperación internacional.

SEXTA.- El Consejo de Europa desde el año 2007 invitó formalmente al gobierno de México a acceder al protocolo de adhesión a la Convención. Sin embargo, hasta ahora el país no ha ratificado formalmente su compromiso de acceder a dicho protocolo puesto que para ello se requiere previamente de una reforma al marco jurídico penal nacional tanto sustantivo como procedimental, así como la creación de CERT's y redes o puntos de contacto 24X7 nacionales para la identificación de conductas penales cometidas a través de Internet. No obstante lo anterior del 31 de marzo al 2 de abril de 2014, tuvo lugar un taller en materia de ciberdelincuencia para América Latina, donde el Estado Mexicano nuevamente se comprometió a impulsar las reformas que harán posible su adhesión al Convenio.

SÉPTIMA.- Las etapas en las que se funda la existencia de un ciberdelito son tres: la de inclusión en los catálogos penales (legislación) la forma en que se debe investigar (forense informática) y la forma en que se acredita ante un juzgado o tribunal (prueba electrónica).

OCTAVA.- En México la legislación procesal penal, es decir en el tema que nos ocupa, el Código Nacional de Procedimientos Penales, no hace referencia a la persecución de conductas cometidas a través de sistemas de cómputo e informáticos, por tanto tampoco específica que autoridades y tribunales deberían ser competentes para investigar, procesar y castigar conductas cometidas a través de sistemas de cómputo e Internet, y por ende, no se establecen procedimientos de cooperación y coordinación entre cuerpos policíales, el Ministerio Público y los Jueces o Tribunales del Poder Judicial que son parte esencial en cualquier procedimiento.

NOVENA.- Contrario a lo que se pudiese pensar acerca de la legislación española en materia de delincuencia cibernética, la misma halla un rezago de consideración, no obstante haber ratificado España en el año 2010 el Convenio del Consejo de Europa sobre el Cibercrimen. Así tenemos que el llamado nuevo Código Penal Español de 1995, únicamente incorporó a los tipos delictivos clásicos a la realidad informática de manera global, es decir, no se creó un Título específico referente a la criminalidad informática, o una legislación especial, como se había hecho en otros países, sino que se optó por una vía intermedia.

DÉCIMA.- No obstante la legislación obsoleta de España, la Policía Nacional y la Guardia Civil, mediante sus respectivas Brigadas de Investigación Tecnológica y Grupo de Delitos Telemáticos han creado sus correspondientes secciones especializadas en la investigación de los delitos de referencia, para lo anterior se han hecho allegar de personal altamente calificado cuyo perfil requiere que cuenten con conocimientos suficientes en informática, técnica procesal penal, experiencia investigadora, relaciones internacionales y cuyo profesionalismo sea cuestionable en ningún momento, dado que la investigación, como todas, empero, tratándose de situaciones complejas, que incluso pueden vulnerar la seguridad de un Estado, como lo es los ataques cibernéticos, se requiere de la absoluta discreción del investigador.

DÉCIMA PRIMERA.- Para combatir los delitos informáticos complejos, caben diversos métodos complementarios a los convencionales:

- Intrusivos (infiltración en la Red criminal a través de agentes encubiertos, obtención de información a través de la interceptación de las comunicaciones con el uso de programas y otros monitorizadores a distancia como los teclados *keylogger*)
- Coercitivos (entradas y registros, detenciones, comiso de ordenadores)
- Disuasorios (uso de delatores y confidentes para los ataques informáticos realizados en grupo organizado)
- Cooperacionistas (la figura del "enlace" con las empresas telefónicas, proveedoras de acceso y prestadoras de servicio de Internet)
- Preventivos (campañas informativas, medidas de restricción del Uso de Internet, auto judicial de alejamiento informático.)
- Legislativos (que específicamente regulen los métodos intrusivos y en concreto la intervención y registro de comunicaciones telemáticas)

DÉCIMA SEGUNDA.- Los ciberataques de contenido son una categoría del grupo de tipologías de cibercrimanilidad, en la que el centro de la infracción lo constituye el contenido que se comunica o se transmite a través de las redes telemáticas, particularmente de la Red de redes, Internet.

PROPUESTA

Concluida la presente investigación y una vez que se ha logrado el objetivo principal de la misma, el cual consistió en demostrar que la ausencia de tipificación de los *ciberdelitos* en México es una limitante en el eficaz desempeño de la función de la policía investigadora, comprobando así que al tener una adecuada tipificación en el marco jurídico respecto de estos delitos, se establecen procedimientos de cooperación y coordinación entre cuerpos policiales, el Ministerio Público y los Jueces o Tribunales del Poder Judicial que son parte esencial en cualquier procedimiento, lo que sin duda, determinará para cada autoridad su nivel de competencia y delimitará su jurisdicción, haciendo con ello que la investigación de estos delitos, a la que podemos denominar informática forense, sea altamente eficaz y por último, que de esta forma se cumplan los requisitos mínimos necesarios en comprobación del delito, refiriéndome a la prueba electrónica.

Dado lo anterior, doy paso a pronunciamiento de la propuesta emitida en relación a la presente investigación, la que se divide en tres etapas:

PRIMERA.- Es indispensable la pronta adhesión del Estado Mexicano al Convenio sobre Ciberdelincuencia del Consejo de Europa o Convenio de Budapest. Para lo cual se propone una reforma integral a los catálogos penales tanto sustantivo como adjetivo, el primero, creando un *Título especial* en el Código Penal Federal, que tipifique, encuadre de manera adecuada e incluso sirva de unificación de criterios para determinar cuál será la denominación correcta en los llamados *ciberdelitos,* y el segundo que aporte los elementos procesales necesarios para la persecución y sanción de dichas conductas.

SEGUNDA.- En segundo término se propone, *no* más creación de policías cibernéticas por parte de las Entidades Federativas, sin legislación que las regule. Rotundamente es urgente la legislación penal en la materia para que con fundamento legal sirva un *modelo único* de policía cibernética, a nivel Federal para la creación de las policías en cada Estado.

TERCERA.- Finalmente se propone *un perfil del policía cibernético*, basado en una profesionalización de la policía, con conocimientos suficientes en informática y a su vez en informática jurídica, técnica procesal penal, experiencia investigadora, facilidad para las relaciones internacionales y ante todo vocación en el servicio.

ANEXOS

Anexo 1

Estructura Orgánica de La Policía Federal

1. Comisionado General

1.1. División de Inteligencia
- 1.1.1. Coordinación de Servicios Técnicos
  - 1.1.1.1. Dirección General del Centro de Monitoreo Técnico
  - 1.1.1.2. Dirección General del Centro de Alertas y Atención de Riesgos
  - 1.1.1.3. Dirección General de Desarrollo y Operación de Coberturas
- 1.1.2. Coordinación de Operaciones Encubiertas
  - 1.1.2.1. Dirección General de Operaciones e Infiltración
  - 1.1.2.2. Dirección General de Reclutamiento y Manejo de Fuentes de Información
  - 1.1.2.3. Dirección General de Supervisión y Vigilancia
- 1.1.3. Coordinación de Análisis y Enlace Internacional
  - 1.1.3.1. Dirección General de Análisis y Estadística
  - 1.1.3.2. Dirección General de Asuntos Policiales Internacionales
  - 1.1.3.3. Dirección General de Indicadores de Integración de la Información

1.2. División de Investigación
- 1.2.1. Coordinación de Investigación de Gabinete
  - 1.2.1.1. Dirección General de Análisis Táctico
  - 1.2.1.2. Dirección General de Fichas y Registros Delictivos
  - 1.2.1.3. Dirección General de Manejo de Crisis y Negociación
- 1.2.2. Coordinación de Investigación de Campo
  - 1.2.2.1. Dirección General de Investigación de Delitos contra la Seguridad e Integridad de las Personas
  - 1.2.2.2. Dirección General de Investigación de Delitos de Alto Impacto
  - 1.2.2.3. Dirección General de Investigación de Delitos Federales
- 1.2.3. Coordinación de Investigación Técnica y Operación
  - 1.2.3.1. Dirección General de Operaciones Técnicas
  - 1.2.3.2. Dirección General de Inteligencia Operativa
  - 1.2.3.3. Dirección General de Apoyo Táctico

1.3. División de Seguridad Regional
- 1.3.0.1. Dirección General de Personal
- 1.3.0.2. Dirección General de Información
- 1.3.0.3. Dirección General de Operaciones
- 1.3.0.4. Dirección General de Logística y Adiestramiento
- 1.3.0.5. Dirección General de Planes y Supervisión
- 1.3.0.6. Dirección General de Control Operativo
- 1.3.0. Coordinaciones Estatales (32)

1.4. División Científica
- 1.4.1. Coordinación para la Prevención de Delitos Electrónicos
  - 1.4.1.1. Dirección General de Prevención de Delitos Cibernéticos
  - 1.4.1.2. Dirección General de Centro Especializado en Respuesta Tecnológica
  - 1.4.1.3. Dirección General de Laboratorios en Investigación Electrónica y Forense
- 1.4.2. Coordinación de Innovación Tecnológica
  - 1.4.2.1. Dirección General de Tecnologías de Información Emergentes
  - 1.4.2.2. Dirección General de Infraestructura e Implementación de Procesos Tecnológicos

1.4.2.3. Dirección General de Innovación y Desarrollo

1.4.3. Coordinación de Criminalística

1.4.3.1. Dirección General de Criminalística de Campo

1.4.3.2. Dirección General de Laboratorios

1.4.3.3. Dirección General de Especialidades

1.5. División Antidrogas

1.5.1. Coordinación de Investigación de Gabinete Antidrogas

1.5.1.1. Dirección General de Análisis Táctico Antidrogas

1.5.1.2. Dirección General de Fichas y Registro de Narcotráfico y Delitos Conexos

1.5.1.3. Dirección General de Enlace y Cooperación Interinstitucional

1.5.2. Coordinación de Investigación de Campo y Técnica Antidrogas

1.5.2.1. Dirección General de Operación Técnica Antidrogas

1.5.2.2. Dirección General de Inteligencia Operativa Antidrogas

1.5.2.3. Dirección General de Apoyo Táctico contra Narcotráfico y Delitos Conexos

1.5.3. Coordinación de Investigación de Recursos de Procedencia Ilícita

1.5.3.1. Dirección General de Análisis Táctico de Delitos contra el Sistema Financiero

1.5.3.2. Dirección General de Inteligencia Financiera para la Prevención

1.5.3.3. Dirección General de Prevención de Operaciones con Recursos de Procedencia Ilícita

1.6. División de Fuerzas Federales

1.6.1. Coordinación de Restablecimiento del Orden Público

1.6.1.1. Dirección General de Fuerzas de Protección

1.6.1.2. Dirección General de Rescate y Apoyo a la Protección Civil

1.6.1.3. Dirección General de Traslados y Apoyo Penitenciario

1.6.2. Coordinación de Reacción y Alerta Inmediata

1.6.2.1. Dirección General de Seguridad Física

1.6.2.2. Dirección General de Reacción y Operación

1.6.2.3. Dirección General de la Unidad Canina

1.6.3. Coordinación de Operaciones Especiales

1.6.3.1. Dirección General de Intervención

1.6.3.2. Dirección General de Explosivos

1.6.3.3. Dirección General de Equipos Especiales

1.7. Secretaría General

1.7.1. Coordinación de Servicios Generales

1.7.1.1. Dirección General de Recursos Humanos

1.7.1.2. Dirección General de Recursos Financieros

1.7.1.3. Dirección General de Recursos Materiales

1.7.2. Coordinación de Operaciones Aéreas

1.7.2.1. Dirección General de Operaciones

1.7.2.2. Dirección General de Mantenimiento

1.7.2.3. Dirección General de Supervisión y Seguridad Aérea

1.7.3. Coordinación de Soporte Técnico

1.7.3.1. Dirección General de Informática

1.7.3.2. Dirección General de Telecomunicaciones

1.7.3.3. Dirección General de Instalaciones Técnicas y Mantenimiento

1.7.4. Coordinación del Sistema de Desarrollo Policial

1.7.4.1. Dirección General de Control de Confianza

1.7.4.2. Dirección General del Servicio Profesional de Carrera y Régimen Disciplinario

1.7.4.3. Dirección General de Formación y Profesionalización

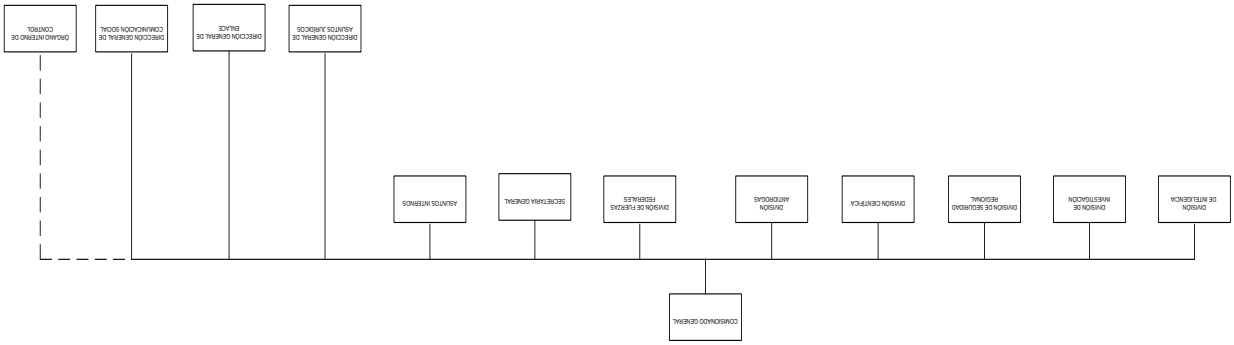
1.8. Asuntos Internos

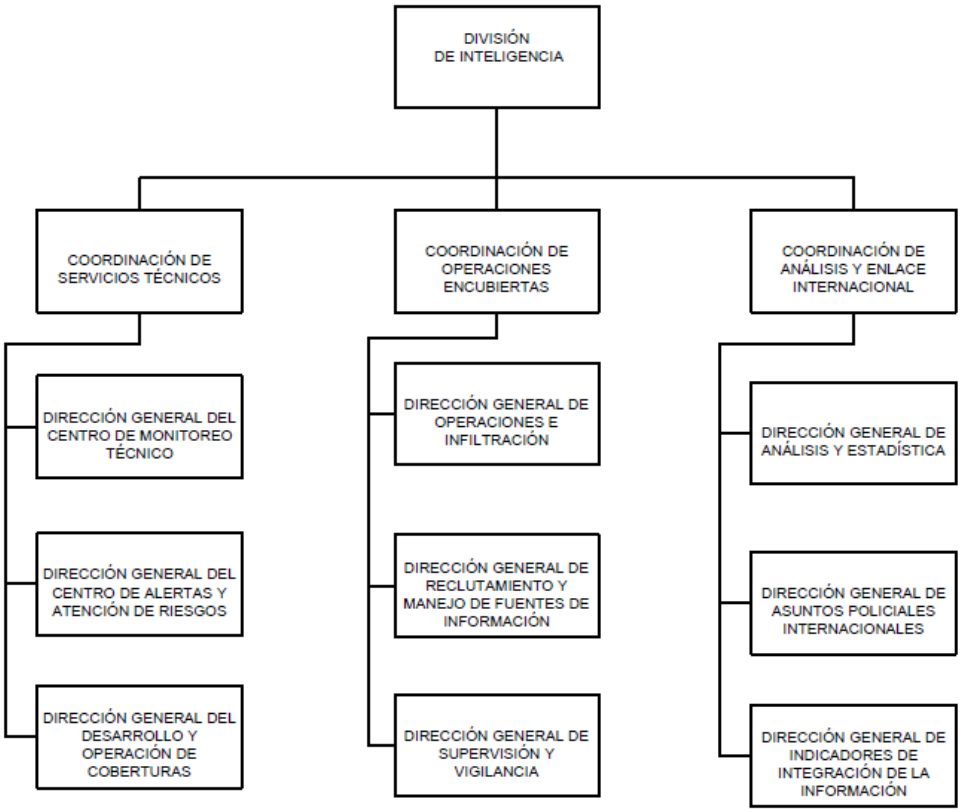
1.8.0.1. Dirección General de Vigilancia y Supervisión Interna

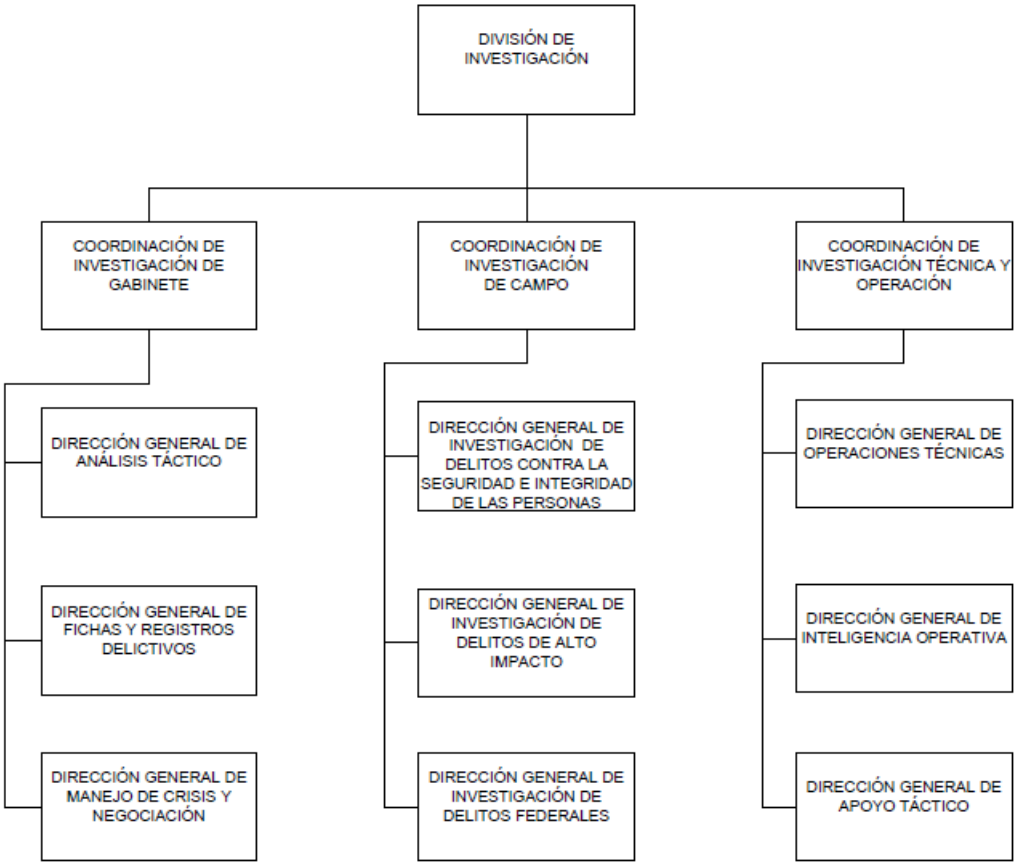
1.8.0.2.	Dirección General de Investigación Interna
1.8.0.3.	Dirección General de Responsabilidades
1.0.0.1.	Dirección General de Asuntos Jurídicos
1.0.0.2.	Dirección General de Enlace
1.0.0.3.	Dirección General de Comunicación Social
1.0.0.4.	Organo Interno de Control

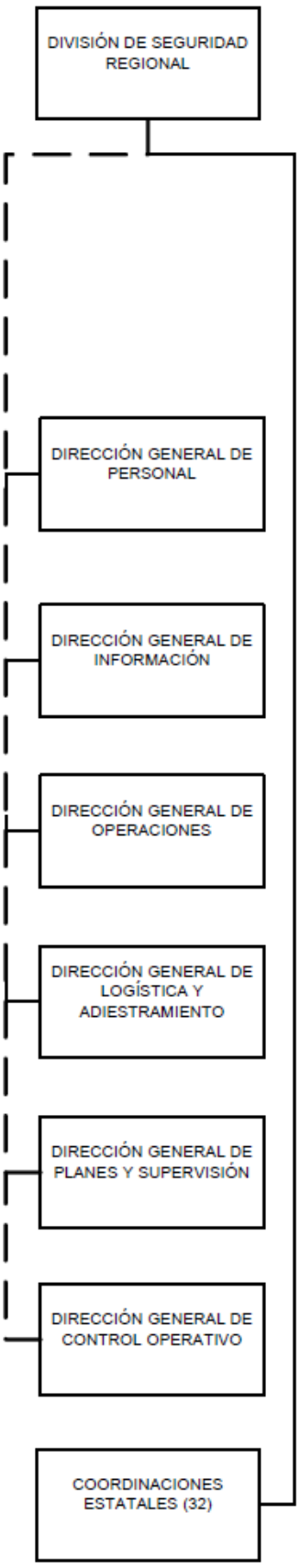
Anexo 2

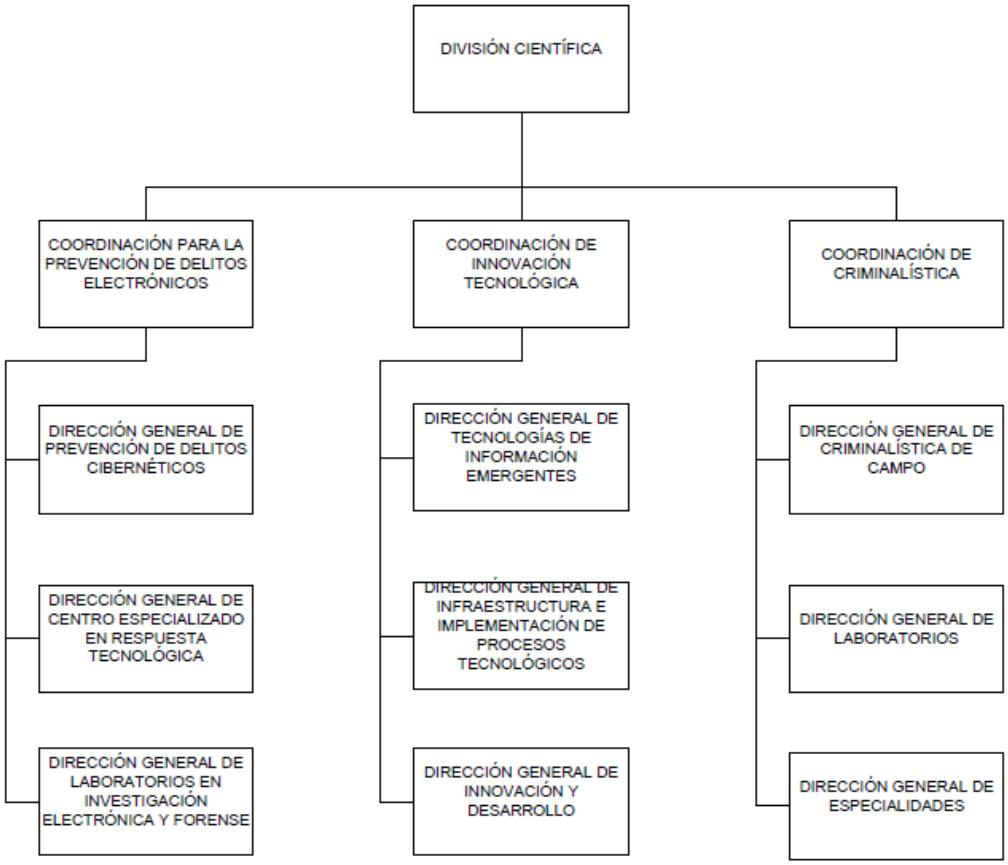
Organigrama de la Policía Federal

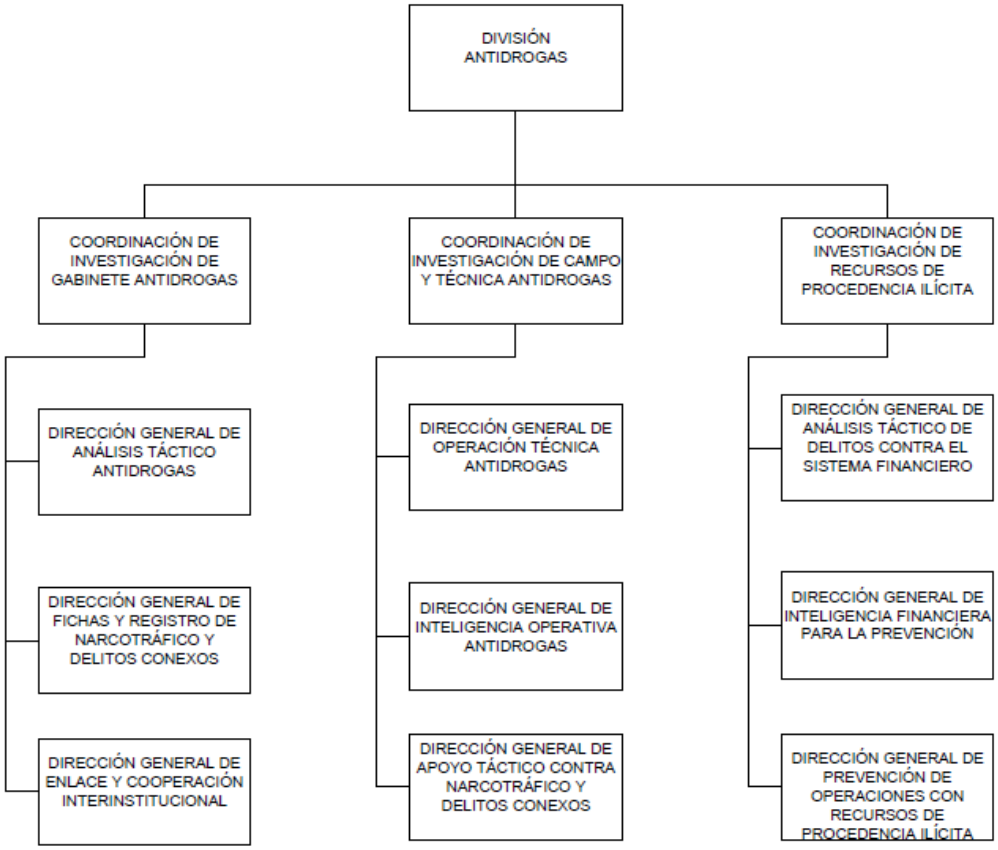


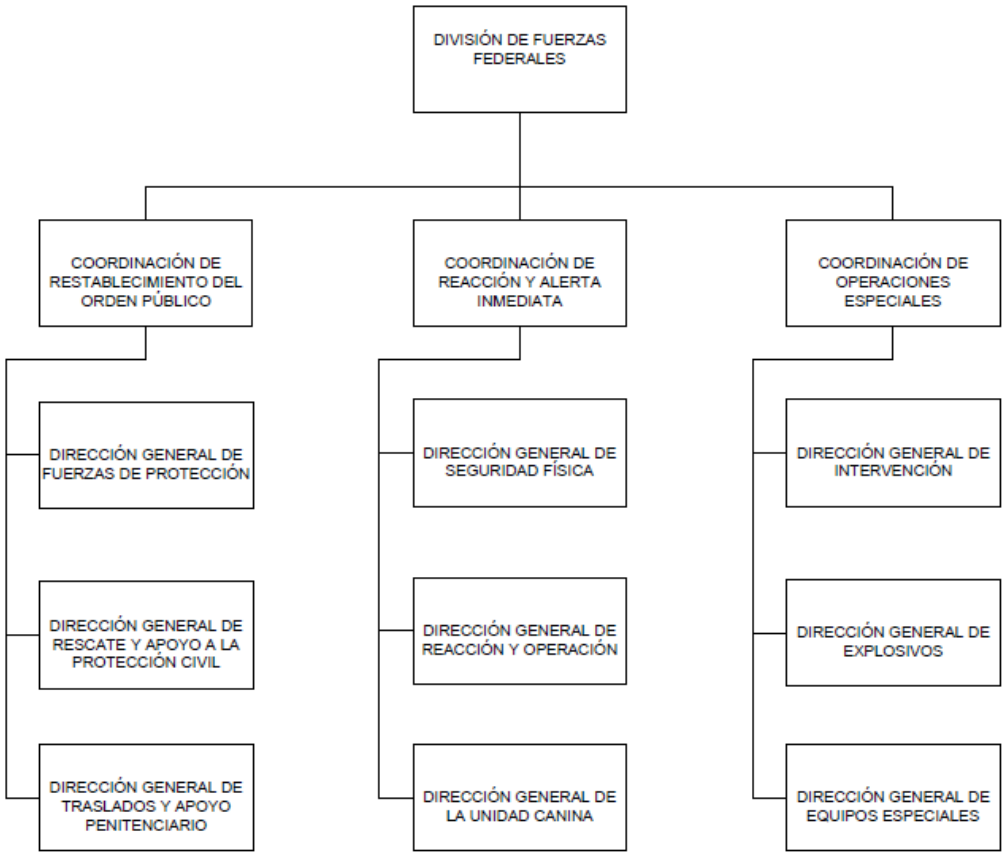

DIVISIÓN DE INTELIGENCIA
COORDINACIÓN DE SERVICIOS TÉCNICOS
COORDINACIÓN DE OPERACIONES ENCUBIERTAS
COORDINACIÓN DE ANÁLISIS Y ENLACE INTERNACIONAL
DIRECCIÓN GENERAL DEL CENTRO DE MONITOREO TÉCNICO
DIRECCIÓN GENERAL DEL CENTRO DE ALERTAS Y ATENCIÓN DE RIESGOS
DIRECCIÓN GENERAL DEL DESARROLLO Y OPERACIÓN DE COBERTURAS
DIRECCIÓN GENERAL DE OPERACIONES E INFILTRACIÓN
DIRECCIÓN GENERAL DE RECLUTAMIENTO Y MANEJO DE FUENTES DE INFORMACIÓN
DIRECCIÓN GENERAL DE SUPERVISIÓN Y VIGILANCIA
DIRECCIÓN GENERAL DE ANÁLISIS Y ESTADÍSTICA
DIRECCIÓN GENERAL DE ASUNTOS POLICIALES INTERNACIONALES
DIRECCIÓN GENERAL DE INDICADORES DE INTEGRACIÓN DE LA INFORMACIÓN

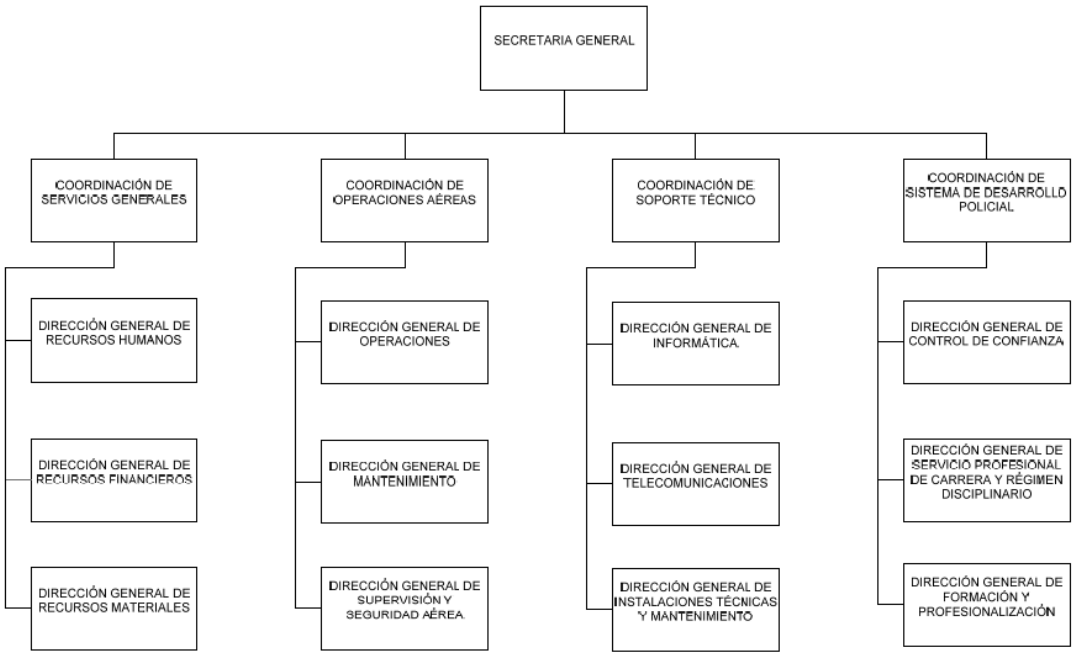

DIVISIÓN DE INVESTIGACIÓN
COORDINACIÓN DE INVESTIGACIÓN DE GABINETE
COORDINACIÓN DE INVESTIGACIÓN DE CAMPO
COORDINACIÓN DE INVESTIGACIÓN TÉCNICA Y OPERACIÓN
DIRECCIÓN GENERAL DE ANÁLISIS TÁCTICO
DIRECCIÓN GENERAL DE FICHAS Y REGISTROS DELICTIVOS
DIRECCIÓN GENERAL DE MANEJO DE CRISIS Y NEGOCIACIÓN
DIRECCIÓN GENERAL DE INVESTIGACIÓN DE DELITOS CONTRA LA SEGURIDAD E INTEGRIDAD DE LAS PERSONAS
DIRECCIÓN GENERAL DE INVESTIGACIÓN DE DELITOS DE ALTO IMPACTO
DIRECCIÓN GENERAL DE INVESTIGACIÓN DE DELITOS FEDERALES
DIRECCIÓN GENERAL DE OPERACIONES TÉCNICAS
DIRECCIÓN GENERAL DE INTELIGENCIA OPERATIVA
DIRECCIÓN GENERAL DE APOYO TÁCTICO


DIVISIÓN DE SEGURIDAD REGIONAL
DIRECCIÓN GENERAL DE PERSONAL
DIRECCIÓN GENERAL DE INFORMACIÓN
DIRECCIÓN GENERAL DE OPERACIONES
DIRECCIÓN GENERAL DE LOGÍSTICA Y ADIESTRAMIENTO
DIRECCIÓN GENERAL DE PLANES Y SUPERVISIÓN
DIRECCIÓN GENERAL DE CONTROL OPERATIVO
COORDINACIONES ESTATALES (32)


DIVISIÓN CIENTÍFICA
COORDINACIÓN PARA LA PREVENCIÓN DE DELITOS ELECTRÓNICOS
COORDINACIÓN DE INNOVACIÓN TECNOLÓGICA
COORDINACIÓN DE CRIMINALÍSTICA
DIRECCIÓN GENERAL DE PREVENCIÓN DE DELITOS CIBERNÉTICOS
DIRECCIÓN GENERAL DE CENTRO ESPECIALIZADO EN RESPUESTA TECNOLÓGICA
DIRECCIÓN GENERAL DE LABORATORIOS EN INVESTIGACIÓN ELECTRÓNICA Y FORENSE
DIRECCIÓN GENERAL DE TECNOLOGÍAS DE INFORMACIÓN EMERGENTES
DIRECCIÓN GENERAL DE INFRAESTRUCTURA E IMPLEMENTACIÓN DE PROCESOS TECNOLÓGICOS
DIRECCIÓN GENERAL DE INNOVACIÓN Y DESARROLLO
DIRECCIÓN GENERAL DE CRIMINALÍSTICA DE CAMPO
DIRECCIÓN GENERAL DE LABORATORIOS
DIRECCIÓN GENERAL DE ESPECIALIDADES


DIVISIÓN ANTIDROGAS
COORDINACIÓN DE INVESTIGACIÓN DE GABINETE ANTIDROGAS
COORDINACIÓN DE INVESTIGACIÓN DE CAMPO Y TÉCNICA ANTIDROGAS
COORDINACIÓN DE INVESTIGACIÓN DE RECURSOS DE PROCEDENCIA ILÍCITA
DIRECCIÓN GENERAL DE ANÁLISIS TÁCTICO ANTIDROGAS
DIRECCIÓN GENERAL DE FICHAS Y REGISTRO DE NARCOTRÁFICO Y DELITOS CONEXOS
DIRECCIÓN GENERAL DE ENLACE Y COOPERACIÓN INTERINSTITUCIONAL
DIRECCIÓN GENERAL DE OPERACIÓN TÉCNICA ANTIDROGAS
DIRECCIÓN GENERAL DE INTELIGENCIA OPERATIVA ANTIDROGAS
DIRECCIÓN GENERAL DE APOYO TÁCTICO CONTRA NARCOTRÁFICO Y DELITOS CONEXOS
DIRECCIÓN GENERAL DE ANÁLISIS TÁCTICO DE DELITOS CONTRA EL SISTEMA FINANCIERO
DIRECCIÓN GENERAL DE INTELIGENCIA FINANCIERA PARA LA PREVENCIÓN
DIRECCIÓN GENERAL DE PREVENCIÓN DE OPERACIONES CON RECURSOS DE PROCEDENCIA ILÍCITA


DIVISIÓN DE FUERZAS FEDERALES
COORDINACIÓN DE RESTABLECIMIENTO DEL ORDEN PÚBLICO
COORDINACIÓN DE REACCIÓN Y ALERTA INMEDIATA
COORDINACIÓN DE OPERACIONES ESPECIALES
DIRECCIÓN GENERAL DE FUERZAS DE PROTECCIÓN
DIRECCIÓN GENERAL DE RESCATE Y APOYO A LA PROTECCIÓN CIVIL
DIRECCIÓN GENERAL DE TRASLADOS Y APOYO PENITENCIARIO
DIRECCIÓN GENERAL DE SEGURIDAD FÍSICA
DIRECCIÓN GENERAL DE REACCIÓN Y OPERACIÓN
DIRECCIÓN GENERAL DE LA UNIDAD CANINA
DIRECCIÓN GENERAL DE INTERVENCIÓN
DIRECCIÓN GENERAL DE EXPLOSIVOS
DIRECCIÓN GENERAL DE EQUIPOS ESPECIALES


SECRETARIA GENERAL
COORDINACIÓN DE SERVICIOS GENERALES
COORDINACIÓN DE OPERACIONES AÉREAS
COORDINACIÓN DE SOPORTE TÉCNICO
COORDINACIÓN DE SISTEMA DE DESARROLLO POLICIAL
DIRECCIÓN GENERAL DE RECURSOS HUMANOS
DIRECCIÓN GENERAL DE RECURSOS FINANCIEROS
DIRECCIÓN GENERAL DE RECURSOS MATERIALES
DIRECCIÓN GENERAL DE OPERACIONES
DIRECCIÓN GENERAL DE MANTENIMIENTO
DIRECCIÓN GENERAL DE SUPERVISIÓN Y SEGURIDAD AÉREA
DIRECCIÓN GENERAL DE INFORMÁTICA
DIRECCIÓN GENERAL DE TELECOMUNICACIONES
DIRECCIÓN GENERAL DE INSTALACIONES TÉCNICAS Y MANTENIMIENTO
DIRECCIÓN GENERAL DE CONTROL DE CONFIANZA
DIRECCIÓN GENERAL DE SERVICIO PROFESIONAL DE CARRERA Y RÉGIMEN DISCIPLINARIO
DIRECCIÓN GENERAL DE FORMACIÓN Y PROFESIONALIZACIÓN


ASUNTOS INTERNOS
DIRECCIÓN GENERAL DE VIGILANCIA Y SUPERVISIÓN INTERNA
DIRECCIÓN GENERAL DE INVESTIGACIÓN INTERNA
DIRECCIÓN GENERAL DE RESPONSABILIDADES

Anexo 3
Protocolos de Internet

Para tener una idea clara del concepto de WWW, es fundamental tener algunas nociones básicas sobre lo que es Internet. Se trata, de una red de redes interconectadas que, gracias a unas normas y estándares comunes pueden comunicarse e intercambiar información todos los ordenadores conectados a dicha red. La arquitectura que da soporte a Internet es la denominada cliente/servidor, esto es, unos ordenadores almacenan la información (los ordenadores servidores) y otros acceden a ella (los ordenadores clientes).

El protocolo más básico de Internet -o paquete de protocolos- es el protocolo TCP/IP *(Transfer Control Protocol/Internet Protocol)*.Cualquier otro protocolo de Internet se basa en IP o le sirve de base.

El funcionamiento del protocolo TCP/IP es el siguiente. Primero, el protocolo TCP (*Transmision Control Protocol)* fragmenta los datos en paquetes de información. Después, estos paquetes son enviados a la red, posiblemente sobre rutas diferentes, según el IP (el Protocolo de Internet). Finalmente, estos paquetes se vuelven a recomponer en el destino (o se restauran en caso de corrupción o pérdida de datos) en su orden correcto de llegada.

Para que sea posible la comunicación entre ordenadores, es necesario que cada máquina posea una identificación única. Así, cada ordenador conectado a Internet tiene un número IP y una DNS *(Domain Name Server)*, el primero se expresa con números y el segundo con letras.

En el contexto de Internet, el ordenador es más que un dispositivo para el cómputo o para el procesamiento de textos, se trata de un instrumento que suministra una plataforma para el sistema operativo y para las aplicaciones de *software* que soportan la transmisión de información en red y su utilización por parte del usuario.

En Internet, las relaciones entre ordenadores siguen comúnmente el modelo de servidor-cliente. Igual que los protocolos TCP/IP, el modelo de servidor-cliente es una característica que homogeniza la comunicación en Internet. Un servidor es un ordenador junto con un *hardware* asociado y las aplicaciones de software que actúan como un depósito para los archivos de la información o los programas de *software*. El servidor envía esta información respondiendo a una petición de los usuarios del *software* cliente a través de la red.

La comunicación de servidor-cliente también sigue un conjunto de protocolos. Estos protocolos definen un uso particular que usan cliente y servidor. Por ejemplo, el protocolo Gopher de Internet, hoy en desuso, definía un uso para estructurar la información en un sistema de menús, submenús y

entradas. Un usuario de un cliente Gopher hacía una petición para obtener una lista de artículos de menú a un servidor Gopher. El servidor Gopher devolvía esta lista y el cliente Gopher mostraba la lista al usuario. En la actualidad, esta misma función la realiza el protocolo HTTP de la World Wide Web.

Los distintos protocolos sirven, pues, para ofrecer una gran variedad de servicios en Internet. Los más utilizados son: la transferencia de archivos, el correo electrónico y el protocolo de la Web, pero existen otros muchos. Cada uno cuenta con aplicaciones clientes que hacen más fácil su uso.

La forma distribuida de servidor-cliente funciona muy eficazmente, ya que el *software* de cliente actúa recíprocamente con el servidor según un protocolo de intercambio de datos estándar. El servidor no tiene que "preocuparse" del *hardware* o las particularidades de *software* del ordenador sobre el que el que reside el *software* del cliente. Por su parte, el *software*del cliente no tiene que "preocuparse" de cómo solicita la información un tipo particular de servidor, puesto que todos los servidores de un protocolo particular se comportan de la misma forma.

Por ejemplo, un cliente de Web que puede tener acceso a cualquier servidor de Web puede ser desarrollado para ordenadores Macintosh. Este mismo servidor de Web podría ser accedido por un cliente de Web soportado sobre un terminal de trabajo Windows que controla un sistema Unix. Esto hace más fácil desarrollar la información porque las versiones de la información distribuida de un servidor no tienen que ser desarrolladas para una plataforma de *hardware* particular. Todas las personalizaciones necesarias para el ordenador del usuario se escriben en el *software* del cliente para aquella plataforma.

El modelo de servidor-cliente es la característica clave para la comunicación en Internet. Un mensaje sobre Internet es codificado, almacenado y transmitido según las reglas de uso del servidor-cliente y el paquete de protocolos TCP/IP.

Para acceder a los archivos concretos dentro de un servidor es necesario conocer dónde están ubicados estos y para ello es preciso dotarlos de una dirección. Esta dirección es la URL o*Universal Resource Locator)* que está compuesta de los siguientes elementos: el protocolo seguido del signo de dos puntos y una doble barra inclinada, nombre de la máquina (número IP o DNS), directorio y subdirectorios, y archivo. Por ejemplo: http://www.hipertexto.info/Internet_tegn.htm

Veamos con más detalle algunos de los conceptos básicos que hay que conocer para comprender Internet:

PROTOCOLOS	OTROS CONCEPTOS BÁSICOS
• TCP/IP • FTP • HTTP • SMTP (mail) • NNTP (news) • IRC • TELNET • GOPHER	• URLs • Direcciones IP • DNS (*Domain Name System*) • Nombres de dominio

PROTOCOLOS

En informática, un protocolo no es más que un conjunto de reglas formales que permiten a dos dispositivos intercambiar datos de forma no ambigua. Un protocolo es, pues, un conjunto de reglas que permiten intercambiar información. El ordenador conectado a una red usa protocolos para permitir que los ordenadores conectados a la red puedan enviar y recibir mensajes, y el protocolo TCP/IP define las reglas para el intercambio de datos sobre Internet. Este conjunto de protocolos, al principio se desarrolló para un proyecto de investigación del Departamento de Defensa de los Estados Unidos, e integra un conjunto de servicios (que incluyen correo electrónico, la transferencia de archivos y la conexión remota) y que puede establecerse entre muchos ordenadores sobre una red local o en redes de un área más amplia.

Las redes conectadas por donde pasa el paquete de protocolos TCP/IP son sumamente robustas. Si una sección de la red (o un servidor de ordenador en la red) se convierte en inoperativo, los datos pueden ser desviados sin causar daño a la red. La homogeneidad del protocolo es la esencia de la comunicación de Internet en el nivel de los datos. Mediante la cooperación de las conexiones de redes y el protocolo TCP/IP pueden conectarse sistemas de comunicación más y más grandes. Las organizaciones individuales pueden controlar su propia red TCP/IP (Internet) y conectarla con otras redes de Internet locales, regionales, nacionales y globales. Internet comparte el paquete de protocolos TCP/IP, sin embargo, Internet no es una red, sino una red de redes, un sistema organizado y distribuido cooperativamente a escala mundial para intercambiar información.

Internet no es la única red global, hay otras redes globales que emplean protocolos diferentes, pero pueden intercambiar datos con Internet mediante puntos de intercambio llamados galerías o *gateways*. La comunicación de redes que no son Internet y que fluye en un punto de entrada es traducida a protocolos de comunicaciones de Internet y reexpedida a su camino, indistinguible de los paquetes que crea TCP enviando un mensaje directamente sobre Internet. De la misma manera, la comunicación puede fluir de Internet a otros puntos de entrada o *gateways* de la misma manera: los

paquetes de Internet son traducidos a los protocolos de no-Internet necesarios para la comunicación sobre la otra red.

El correo electrónico es una forma popular de comunicación que se realiza a través de estas galerías o *gateways*. Mediante las *gateways* de correo electrónico, los usuarios sobre Internet pueden intercambiar correo electrónico con otros usuarios sobre redes que no son de Internet, como las que se utilizaban en los primeros tiempos de la red como BITNET (*Because Its Time Network*), UUCP (*Unix-Unix Copy Protocol*), y FidoNet (red basada en la comunicación de PCs sobre líneas telefónicas). Los usuarios de Internet también pueden intercambiar correo electrónico con muchos servidores. El resultado es que el correo electrónico se disemina libremente en todas partes de Internet, así como en muchas otras redes. La colección resultante de redes mundiales que intercambian correo electrónico ha sido denominada *Matrix*.

Aunque el flujo libre de correo electrónico haga difícil la distinción entre la comunicación de Internet y la comunicación de no-Internet en *Matrix*, la distinción entre Internet y *Matrix* para muchas otras formas de comunicación es crucial. Por ejemplo, la comunicación que usaba el protocolo Gopher de Internet no puede ser compartida fácilmente fuera de Internet. Asimismo Telnet, FTP (el Protocolo de Transferencia de Archivos) y la comunicación de World Wide Web está restringida, en la mayor parte de casos, a los usuarios de Internet. Los servicios comerciales en línea, reconociendo el valor de acceso a Internet para sus clientes, han estado creando más clases de entradas (*gateways*) a Internet que permiten a sus usuarios tener acceso a Telnet, FTP y la World Wide Web en Internet.
El resultado de esta mezcla de redes globales ha hecho que el protocolo de Internet se convierta en una especie de lengua franca del ciberespacio, creando puntos en común con otras muchas redes en línea que se unen mediante las susodichas *gateways*.

Los protocolos TCP/IP permanecieron bajo secreto militar hasta 1989. La World Wide Web llegó en 1991.Los protocolos son, pues, una serie de reglas que utilizan los ordenadores para comunicarse entre sí. El protocolo utilizado determinará las acciones posibles entre dos ordenadores. Para hacer referencia a ellos en el acceso se escribe el protocolo en minúsculas seguido por "://". Por ejemplo: http://www.hipertexto.info, ftp://ftp.hipertexto.info, etc.

Protocolos más habituales:

TCP/IP. Tansmision Control Protocol/Internet Protocol:

Transmision Control Protocol o Protocolo de Control de Transmisión fragmenta los datos en paquetes de información. Después, estos paquetes son enviados a la red, posiblemente sobre rutas diferentes. El IP es el protocolo más básico de Internet, y provee todos los servicios necesarios para el transporte de datos. Cualquier otro protocolo de Internet se basa en IP o le sirve de base.

Fundamentalmente IP provee:

- **Direccionamiento:** Las cabeceras IP contienen las direcciones de las máquinas de origen y destino (direcciones IP), direcciones que serán usadas por los enrutadores (*routers*) para decidir el tramo de red por el que circularán.
- **Fragmentación:** Si la información a transmitir ("datagramas") supera el tamaño máximo "negociado" (MTU) en el tramo de red por el que va a circular podrá ser dividida en paquetes más pequeños, y reensamblada luego cuando sea necesario.
- **Tiempo de Vida de Paquetes:** Cada paquete IP contiene un valor de Tiempo de Vida (TTL) que va disminuyendo cada vez que un enrutador recibe y reenvía el paquete. Cuando este valor llega a ser de cero, el paquete deja de ser reenviado (se pierde).
- **Tipo de Servicio:** Este es un valor sin definición previa pero que puede indicar, por ejemplo, la prioridad del paquete.
- **Otras opciones:** Valores sin contenido definido previamente que se pueden utilizar, por ejemplo, para que la máquina de origen especifique la ruta que debe seguir el paquete, o para que cada enrutador agregue su propia dirección (para realizar seguimiento de ruta), o para indicar opciones de seguridad de la información contenida, etc.

El IPv6 será la próxima generación de protocolos de Internet y ya está en marcha. Este protocolo se ha desarrollado para ampliar la capacidad de conexión debido al crecimiento de dispositivos y al aumento de equipos portátiles. Y así, ofrecerá la infraestructura necesaria para teléfonos móviles, agendas PDA, electrodomésticos, etc.

La mayor diferencia entre la versión de IP utilizada actualmente (IP versión 4) e IPv6 radica en el espacio de direcciones más grande que admite IPv6. IPv6 admite direcciones de Internet de 128 bits, mientras que IP (versión 4) lo hace a 32 bits, además de ofrecer una configuración más simple y una mayor seguridad.

Por su parte, el protocolo TCP proporciona un servicio de comunicación que forma un circuito, es decir, hace fluir los datos entre el origen y el destino para que sea continuo. Este circuito virtual es lo que se denomina conexión. Así, TCP conecta los ordenadores o programas -loa llamados y los que llaman-, chequea los errores, controla el flujo y tiene capacidad para interrumpirlos.

FTP

File Transfer Protocol o Protocolo de transferencia de archivos . Es un protocolo que define cómo transferir archivos de un ordenador a otro, de un servidor remoto a un servidor local o viceversa. Se precisa un servidor de FTP y un cliente de FTP. Los servidores pueden ser de libre acceso con

un *login* o FTP anónimo. El FTP anónimo es un servidor público de FTP al cual tiene acceso cualquier usuario de Internet sin necesidad de utilizar ninguna contraseña. Se puede utilizar desde un navegador web aunque hay programas específicos comoCuteFTP. La mayoría de las páginas web son "subidas" a los servidores respectivos utilizando este protocolo para transferir los archivos desde el ordenador que ha confeccionado las páginas web hasta el servidor.

HTTP

HyperText Transfer Protocol o Protocolo de Transferencia de Hipertextos. Es el protocolo utilizado por los servidores de la World Wide Web desde el nacimiento de la Weben 1990. El protocolo HTTP es el que permite el intercambio de información hipertextual (enlaces) de las páginas web. Se trata de un protocolo genérico orientado a objetos, que puede usarse para muchas tareas como servidor de nombres y sistemas distribuidos orientados a objetos, por extensión de los comandos o los métodos usados. Una de sus características principales es la independencia en la visualización y presentación de los datos, lo que permite que los sistemas sean construidos independientemente del desarrollo de nuevos avances en la representación de los datos. Para visualizar los datos de la Web se precisa de un navegador instalado en la máquina del ordenador cliente. En este protocolo existen una serie de conceptos tales como:

- Conexión: es el circuito virtual establecido entre 2 programas en una red de comunicación
- Mensaje: es la unidad básica de un protocolo HTTP y consiste en una secuencia estructurada que se tramite entre los programas
- Cliente: es el programa que hace la llamada al servidor y es el que atiende en la transmisión la trama de los mensajes
- Servidor: es el programa que presta el servicio en la red
- Proxy: se trata de un programa intermedio que actúa sobre el servidor y el cliente

Así, pues, el protocolo HTTP se basa en la conexión entre cliente y servidor. Una transacción HTTP consiste básicamente en:

- Conexión: establecimiento de una conexión del cliente con el servidor. El puerto TCP/IP 80 es el puerto más conocido, pero se pueden especificar otros puertos no reservados.
- Solicitud: envío por parte del cliente de un mensaje de solicitud al servidor.
- Respuesta: envío por parte del servidor de una respuesta al cliente.
- Cierre: fin de la conexión por parte del cliente y el servidor.

SMTP (mail)

EL SMTP *Simple Mail Transfer Procol* o Protocolo de Transmisión de Correo Simple es el protocolo que nos permite recibir correos electrónicos y, junto con el protocolo POP (*Post Office Protocol)* o Protocolo de Oficina de Correos, usado por los ordenadores personales para administrar el correo

electrónico, nos permitirá bajarnos los mensajes a nuestro ordenador. Para la mensajería instantánea se usa ahora el protocolo IMAP *Internet Messagins Access Protocol* (Protocolo de mensajería instantánea en Internet), más sofisticado que el protocolo POP.

NEWS (NNTP)

Network News Tranfer Protocol. Protocolo de transferencia de sistemas de redes de *news* o noticias. Se trata de un foro de discusión por temas en forma de tablón de anuncios que cuenta con sus propios servidores y sus propios programas. Generalmente, el mismo programa que gestiona correos electrónicos, sirve para gestionar las *news* o noticias.

IRC

IRC o *Internet Relay Chat* es un protocolo de comunicación que permite conversaciones (*chats*) y debates en grupo o en privado, en tiempo real siguiendo la arquitectura del modelo cliente-servidor, pero formándose redes entre los servidores para acoger a más usuarios. Las conversaciones se desarrollan en los denominados canales de *chat*. Se entra en ellos adoptando un *nickname* o apodo y existen personas encargadas de crear y mantener los canales (los llamados CS o Chan Service), personas encargadas de mantener la red (IRCop), usuarios con privilegios de administrador del canal (Op) e incluso robots (Bot) que automatizan los servicios del canal. Existen muchos servidores de IRC. Algunos de ellos son: irc.

Para acceder a uno de estos servicios como usuario se requiere de un programa o cliente de IRC. Actualmente este servicio también se presta a través de la interfaz de la World Wide Web y existen también otros programas de mensajería integral que permiten conjuntamente prestaciones de mensajería rápida, correo electrónico, audioconferencia, videoconferencia, asistencia remota y otras prestaciones.

TELNET

Protocolo que permite la conexión remota a otro ordenador y que permite manejarlo como si se estuviese físicamente ante él. Así, es posible arreglar fallos a distancia o consultar datos en la otra máquina.

Ha sido un sistema muy utilizado por las grandes bibliotecas y centros de documentación como modo de acceso a sus catálogos en línea. Sin embargo, dejó de usarse hace unos años, cuando apareció y se popularizó el SSH (*Secure Shell*), que puede describirse como una versión cifrada de telnet. Uno de los mayores problemas de TELNET era la seguridad, ya que los nombres de usuario y contraseñas viajaban por la red sin cifrar. Para que la conexión funcionara, la máquina a la que se

accede debía tener un programa especial que recibía y gestionaba las conexiones. El programa, al igual que el protocolo, también se denomina TELNET.

GOPHER

Es un sistema de entrega de información distribuido que hoy se ha dejado de utilizar. Utilizando gopher era posible acceder a información local o bien a servidores de información gopher de todo el mundo. Permitía establecer una jerarquía de documentos, y búsquedas en ellos por palabras o frases clave. Su nombre se debe a la mascota -un topo- de la Universidad de Minessotta, donde fue creado, aunque otros autores sugieren que es una deformación de la frase *goes-fer* (busca). Fue el precursor de la Web al resolver el resolver el problema de cómo ubicar los recursos en Internet reduciendo todas las búsquedas a menús y submenús.

OTROS CONCEPTOS BÁSICOS

URLs (Unit Resource Locator)

La dirección completa de una página web se denomina URL (*Uniform Resource Locator*) o localizador uniforme de recursos, mientras que la dirección del servidor se conoce como DNS (*Domain Name System*) o nombre de dominio.

La URL no es más que la dirección electrónico para poder acceder a un recurso en un servidor remoto. El tipo más común de URL es el de las páginas web, con la dirección http:// , pero existen otras direcciones URL como ftp://, que proporciona la ubicación de red de un recurso FTP para poder transferir archivos, y existen otros muchos tipos de recursos. Los siguientes esquemas son algunos reconocidos por la RFC (Request For Comments) *y* aprobados por la Internet Society (ISOC):

- ftp - "File Transfer protocol"
- http - "HyperText Transfer Protocol"
- gopher - El protocolo Gopher
- mailto - Dirección de Correo Electrónico
- news - "USENET news"
- nntp - "USENET news" usando acceso NNTP
- telnet - Sesiones interactivas
- wais - "Wide Area Information Servers"
- file - Nombres de fichero específicos de un host

Como para visualizar las páginas web se emplea el protocolo HTTP (Hypertext Transfer Protocol), normalmente los navegadores asumen por defecto el protocolo HTTP y no es necesario teclear http:// al introducir las direcciones URL, sin embargo, como ya hemos afirmado, también se emplean otros protocolos como el FTP.

Los nombres pueden ser muy largos o muy sencillos, dependiendo de la ruta de los directorios y subdirectorios que hay que seguir para localizar la página: Protocolo/Nombre de dominio internacional/Directorio/Subdirectorio/Subdirectorio/Archivo

Hablamos de una URL absoluta cuando la dirección completa de Internet correspondiente a una página o recurso de la World Wide Web. La dirección URL absoluta incluye un protocolo, como "http", una ubicación en la red y una ruta de acceso y un nombre de archivo opcionales. Por ejemplo, http://www.hipertexto.info es una dirección URL absoluta. Veamos una URL desglosada: http://www.hipertexto.info/documentos/hipertexto.htm

DNS (Domain Name System)

La DNS (*Domain Name System*) o sistema de nombres de dominio es el que permite localizar una dirección en Internet. En realidad, el sistema de nombres de dominio se creó para facilitar la navegación, pues no es más que el alias de las direcciones IP, que al constar de grupos de cuatro números son difíciles de recordar. Cada dirección IP tiene, pues, asignado un nombre de dominio.
Dirección IP: 121.120.10.1
DNS: www.hipertexto.info (Se trata de un ejemplo ficticio)

La DNS consiste en una serie de tablas de equivalencias entre dominios y direcciones IP. Estas tablas están distribuidas por servidores repartidos en Internet y que se actualizan de forma continua. Los ordenadores permanentemente conectados a Internet (los servidores) tienen direcciones fijas, pero los que se conectan de forma ocasional (clientes) reciben una dirección IP de forma ocasional cada vez que se conectan por parte de sus respectivos servidores. Las palabras que forman un nombre de dominio responden a una jerarquía organizada de derecha a izquierda: Dominio 3er nivel. Dominio de 2º nivel. Dominio de 1er nivel

Nombres de dominio

Dominios de primer nivel:	***Dominios geográficos:***

• **com** para compañías y empresas comerciales • **net** para organizaciones relacionadas con Internet • **org** para organizaciones que no se pueden clasificar en ninguna otra categoría • **edu** para instituciones educativas (sólo lo suelen utilizar las universidades de EE.UU.) • **gov** para el gobierno de EE.UU. • **mil** para las Fuerzas Armadas de EE.UU. • **biz** para negocios y empresas comerciales • **info** para proveedores de servicios de información • **name** para páginas personales	• **es** España • **fr** Francia • **uk** Reino Unido • **ca** Canadá • **it** Italia • **eu** Unión Europea • **mx** México (existen unos 260 dominios de tipo geográfico).

*Fuente de consulta: *http://www.hipertexto.info/documentos/Internet_tegn.htm*

Anexo 4

El caso Gürtel

2009

6 de febrero: La Audiencia Nacional, por orden del juez Baltasar Garzón, abre una investigación por una supuesta trama de corrupción que operaba en Madrid, Valencia y la Costa del Sol. A los implicados se les acusa de blanqueo de capitales, fraude fiscal, cohecho y tráfico de influencias. Comienzan a surgir los vínculos de los detenidos con el Partido Popular (PP), uno de los cinco detenidos es un empresario muy ligado al Ayuntamiento de Boadilla del Monte, del Después de sabría que el detenido es Francisco Correa, al que se considera cabecilla de la supuesta red corrupta.

8 de febrero: Salen a la luz en distintos medios de comunicación los nombres de algunos de los miembros del PP presuntamente implicados en la trama: Arturo González Panero, alcalde de Boadilla del Monte; Guillermo Ortega, gerente del Mercado Puerta de Toledo en Madrid; y Alberto López Viejo, consejero de Deportes de la Comunidad de Madrid.

10 de febrero: Garzón amplía su auto y ya son 37 los imputados en la presunta trama. El PP se queja ante el juez de la Audiencia por las filtraciones del sumario que llegan a la prensa y 24 horas después pide la recusación del juez y anuncia el fin del pacto de la Justicia firmado por el Gobierno al conocerse que el entonces ministro Bermejo coincidió con Garzón en una cacería sólo un día después de que saliera a la luz la operación de la Audiencia Nacional.

12 de febrero: Garzón manda a prisión a tres de los detenidos por la presunta trama corrupta: Francisco Correa, Pablo Crespo y Antoine Sánchez. El juez los acusa de delitos de blanqueo de capitales, tráfico de influencias, defraudación y cohecho. Por otro lado, queda en libertad Álvaro Pérez Alonso.

5 de marzo: Tras las peticiones de la Fiscalía y el PP, y los indicios hallados contra aforados (diputados, senadores y otros altos cargos políticos que no pueden ser juzgados por la Audiencia Nacional), el juez Garzón se inhibe del caso 'Gürtel' y cede la investigación de la presunta trama a los tribunales superiores de Valencia y Madrid. El juez amplía las imputaciones a otros seis miembros del PP

17 de marzo: Los tres únicos imputados encarcelados por el 'caso Gürtel' -el líder de la supuesta trama, Francisco Correa, y sus presuntos colaboradores Antoine Sánchez y Pablo Crespo- acuden a la Audiencia Nacional para abrir su correspondencia ante el juez Baltasar Garzón. La ley permite al magistrado aplicar esta medida para saber si en las cartas recibidas en la cárcel hay algo de interés para su investigación.

27 de marzo: Baltasar Garzón imputa a otras diez personas en la llamada 'Operación Gürtel', con lo que el número de imputados se eleva a 55.

24 de junio. El Tribunal Supremo asume la investigación del tesorero del PP Luis Bárcenas y el diputado Jesús Merino, pero descarta hacerse cargo de todo el 'caso Gürtel'.

2010

25 de marzo. *El Tribunal Superior de Justicia de Madrid anula las escuchas grabadas en la cárcel y ordenadas por el Juez Garzón entre los imputados y sus abogados.*

5 de abril. El juez exige más de 200 millones de fianza a Correa y a sus colaboradores en "Gürtel".

1o de mayo. *Baltasar Garzón asegura al juez que "las escuchas eran la única vía para no perder los fondos del Gürtel".*

18 de noviembre. *El Tribunal Supremo deniega las pruebas solicitadas por el juez Baltasar Garzón en la causa que le investiga por ordenar las escuchas a los imputados en el caso Gürtel en prisión y sus abogados. Considera que esas diligencias no son esenciales ni imprescindibles.*

2012

12 de enero. *El jurado escucha diferentes conversaciones telefónicas grabadas por la Policía, en una de ellas, grabada el 7 de enero de 2009.*

11 de junio. El presunto cabecilla de la trama Gürtel, Francisco Correa, sale de prisión después de que su abogado haya depositado la fianza de 200.000 euros que le impuso el juez Pablo Ruz para abandonar la cárcel de Soto del Real (Madrid), en la que ingreso en febrero de 2009

7 de mayo. *El juez Pablo Ruz, por orden de la sección cuarta de lo Penal de la Audiencia Nacional, deberá pronunciarse sobre la legalidad de las escuchas aportadas por el exconcejal de Majadahonda (Madrid) José Luis Peñas que dieron origen al 'caso Gürtel', tal y como pidieron los imputados Francisco Correa y Ricardo Galeote, alegando que se había vulnerado su intimidad.*

> La Agencia Española de Protección de Datos se suma a las instituciones que, como el Tribunal Supremo en una decena de sentencias, han respaldado sin fisuras el sistema de escuchas denominado. Sistema Integral de Intercepción de Telecomunicaciones, Sitel) y que, después de ser utilizado para desmontar la trama de corrupción en el ‘caso Gurtel’, es criticado por considerarlo “ilegal e inconstitucional”. Las principales conclusiones del informe realizado por la agencia después de

inspeccionar tanto a operadoras de telecomunicaciones como miembros de los cuerpos y fuerzas de seguridad son:

Autorización Judicial. La incorporación de datos del Sitel sólo es posible cuando la operadora que presta el servicio a la línea objeto de interceptación, una vez recibida y analizada la autorización judicial, activa dicha inclusión. El tratamiento de datos en Sitel se produce siempre bajo el control de la autoridad judicial. Asimismo, la información contenida en Sitel que da bajo control judicial.

Acceso por la policía. La actividad de los cuerpos y fuerzas de seguridad queda enmarcada dentro de las funciones de la Policía Judicial previstas en las Leyes, y, en consecuencia el acceso se efectúa en los términos previstos por el juez y para la investigación concreta a que se refiere la autorización. Así documentó el diario *El País*.

2013

11 de febrero. *La Audiencia Nacional avala las diligencias de investigación en el 'caso Gürtel' (como pinchazos telefónicos y registros) porque no guardan relación con las escuchas ordenadas por el juez Baltasar Garzón que fueron declaradas nulas y que le costaron una condena de 11 años de inhabilitación.*

18 de febrero. *Un informe pericial verifica la autenticidad de las grabaciones que dieron origen al 'caso Gürtel', registradas por el exconcejal del PP de Majadahonda José Luis Peñas y en las que aparece el presunto cabecilla de la trama, Francisco Correa.*

25 de febrero. El Tribunal Supremo informa al Gobierno en contra de la petición de indulto del exjuez de la Audiencia Nacional Baltasar Garzón debido, dice el tribunal, a que no concurren circunstancias de justicia y equidad que lo aconsejen, ya que el penado no se ha arrepentido.

11 de marzo. El juez Ruz vuelve a citar a los presuntos cabecillas de la trama en el marco de las diligencias previas a cerrar el caso. Se trata de Francisco Correa, Pablo Crespo, Álvaro Pérez 'El Bigotes' y el contable José Luis Izquierdo.

FUENTES DE CONSULTA

BIBLIOGRAFÍA

ANDRÉS MARTÍNEZ, Gerónimo Miguel, *Derecho de policía (policiología y seguridad pública),* México, Flores Editor y Distribuidor, 2010, 1170 pp.

ARILLA BAS, Fernando, *Derecho Penal,* 2ª ed., México, Porrúa, 2011, 350 pp.

ARMAZA ARMAZA, Emilio José (coord.), *La adaptación del derecho penal al desarrollo social y tecnológico,* Granada España, Ed. Comares, 614 pp.

AZAOLA CALDERÓN, Luis, *Delitos informáticos y Derecho penal,* México, Editorial UBIJUS, 2010, 110 pp.

BERGMAN, Marcelo, *Seguridad Pública y Estado en México, análisis de algunas iniciativas,* 2ª ed., México, Editorial Fontamara, 2011, 155 pp.

CAMPOLI Gabriel Andrés, *Derecho Penal Informático en México,* México, INACIPE, 2004, 116 pp.

------, *Delitos informáticos en la legislación mexicana,* México, INACIPE, 2007, 175 pp.

CASTELLANOS TENA, Fernando, *Lineamientos elementales de Derecho Penal,* 27 ed., México, Porrúa, 1989 pp.

CRUZ TORRERO, Luis Carlos, *Seguridad Pública,* 2ª ed., *México*, Editorial Trillas, 2007, 300 pp.

DESIMONI, Luis María, *Prevención policial y prueba en materia penal,* Argentina, Editorial Policial, 1995, 235 pp.

DÍAZ-ARANDA, Enrique, *Derecho Penal Parte General,* 3° ed., México, Porrúa, 2012, 421 pp.

GARCÍA RAMÍREZ, Sergio, *Derecho Penal,* 3ª ed., México, Porrúa, 2007, pp. 271.

GÓMEZ DEL CAMPO DÍAZ BARREIRO, Bernardo, *En búsqueda de un perfil policial mexicano,* México, Porrúa, 2010, 516 pp.

JIMÉNEZ MARTÍNEZ, Javier, *La Teoría del Delito, Aproximación al Estado de la Discusión,* México, Porrúa, 2010, 1317 pp.

LOZANO TOVAR, Eduardo, *Seguridad Pública y Justicia, una visión político criminológica integral,* México, Porrúa, 2009, 190 pp.

MALDONADO SÁNCHEZ, Isabel, *La Policía en el Sistema Penal Acusatorio, investigación científica del delito y custodia de la evidencia,* 2ª ed., México, Palacio del Derecho Editores, 2010, 140 pp.

MALO CAMACHO, Gustavo, *Derecho Penal Mexicano,* 7ª ed., México, Porrúa, 2010, 1025 pp.

MARTÍNEZ GARNELO, Jesús, *La policía nacional investigadora del delito,* 2ª ed., México, Porrúa, 2003, 36 pp.

------ *Sistema Nacional de Seguridad Pública,* 2ª ed., México, Editorial Porrúa, 2012, 1123 pp.

MARTÍN GARCÍA, Pedro, *La actuación de la policía judicial en el proceso penal,* Madrid, MARCIAL PONS, 2006, 392 pp.

MIRÓ LLINARES, Fernando, *El cibercrimen, fenomenología y criminología de la delincuencia en el ciberespacio,* Madrid, Marcial Pons, 2012, 336. pp.

NAVA GARCÉS, Alberto Enrique, *Análisis de los delitos cibernéticos,* México, Porrúa, México, 2005, 119 pp.

------, *El Derecho en la era digital*, México, Porrúa, 2013, 204 pp.

------, *La prueba electrónica en materia penal,* México, Porrúa, 2011, 236 pp.

ORELLANA WIARCO, Octavio A., *Seguridad pública, profesionalización de los policías,* México, Porrúa, 2010, 190 pp.

ORTIZ PRADILLO, Juan Carlos, *Problemas procesales de la Ciberdelincuencia*, Madrid, Ed. Colex, 2013, 256 pp.

PAVÓN VASCONCELOS, Francisco, *La Causalidad en el delito,* 5ta ed., México, Porrúa, 2004, 178 pp.

POLINA LEÓN, José Gerardo, *La Seguridad Pública entre la racionalidad y el Caos,* México, Editorial Porrúa, 2007, 396 pp.

RABASA GAMBOA, Emilio, *El marco jurídico de la Seguridad Pública en México,* México, Porrúa, 2012, 218 pp.

RAMÍREZ RAMÍREZ, Efrén, *La ética en la formación de la Policía, manual de capacitación,* México, Porrúa, 2009, 187 pp.

------, *Los Derechos Humanos, en la formación de la Policía Judicial, manual de capacitación,* México, Porrúa, 2009, 152 pp.

SUÁREZ DE GARAY, María Eugenia, *Los policías: una averiguación antropológica,* México, ITESO, 2006, 487 pp.

TELLEZ VALDÉS, Julio, *Derecho Informático,* 4ta ed., México, Editorial Mc Graw Hill, 2008, 636 pp.

TORRES BRAVO, Sergio Ibán, *Perspectiva general de la seguridad pública,* México, s.e., 2013, 69 pp.

VÁZQUEZ AZUARA, Carlos Antonio, *Combate a la delincuencia cibernética,* México, Editorial Universidad de Xalapa, 2012, 323 pp.

VELASCO NÚÑEZ, Eloy, *Delitos cometidos a través de Internet, cuestiones procesales,* Madrid, Ed. La Ley, 2010, 340 pp.

VELASCO SAN MARTÍN, Cristos, *La jurisdicción y competencia sobre delitos cometidos a través de sistemas de cómputo e Internet,* México, Tiran lo Blanch, 2012, 414 pp.

YAÑEZ ROMERO, José Arturo, *Policía Mexicana,* Plaza Valdés Editores, México, 1999, 293 pp.

ZÚÑIGA RODRÍGUEZ, Laura, *et al. Derecho Penal, Sociedad y Nuevas Tecnologías,* Salamanca, España, Ed. Colex, 2001, 280 pp.

LEGISLACIÓN

Diario Oficial de la Federación

Código Nacional de Procedimientos Penales

Código Penal Federal
Constitución Política de los Estados Unidos Mexicanos
Boletín Oficial del Estado (España)
Ley de Enjuiciamiento Criminal (España)
Ley General de Telecomunicaciones (España)
Ley Orgánica de Protección del Tratamiento Automatizado de los Datos de Carácter Personal (España)
Ley Orgánica del Poder Judicial (España)
Ley Orgánica del Poder Judicial del Estado
Nuevo Código Penal de 1995 (España)

HEMEROGRAFÍA

ADÁN DEL RÍO, Carmen*, La persecución y sanción de los delitos informáticos*, revista EGUZKILORE, número 20, diciembre de 2007.

CORCOY BIDASOLO, Mirentxu, "Problemática de la Persecución Penal de los denominados delitos Informáticos: Particular referencia a la participación criminal y al ámbito espacio temporal de comisión de los hechos", revista EGUZKILORE, número 21, año 2007.

IGLESIAS, Gonzalo, "El problema de la investigación de los delitos informáticos", *Revista Digital de la Red Iberoamericana de Derecho informático,* Argentina, núm. 13, diciembre de 2012.

REQUENA HIDALGO, Jesús, "De la sociedad disciplinaria a la sociedad de control: la incorporación de nuevas tecnologías a la policía" *Scripta nova, revista electrónica de geografía y ciencias sociales,* España, vol. VIII, núm. 170 (43), 1 de agosto de 2004.

VALENZUELA ARGÜELLES, Rebeca, “Las redes sociales y su aplicación en la educación*”, Revista Digital Universitaria,* México, volumen 14, núm. 4, 1 de abril de 2013.

FUENTES ELECTRÓNICAS

ASOCIACIÓN MEXICANA DE INTERNET A.C., “Estudio MKT digital y redes sociales”, en *https://www.amipci.org.mx/estudios/otros_estudios/MKT_Digital_y_Redes_Sociales_en_M%C3%A9xico_2013.pdf* (Consultado: 24 de julio de 2014)

CÁMARA DE DIPUTADOS, en *http://www.diputados.gob.mx/LeyesBiblio/pdf/CNPPpdf* (Consultado: 12 de enero de 2013)

CASSOU RUIZ, Esteban, “Delitos informáticos en México” en: *http://www.ijf.cjf.gob.mx/publicaciones/revista/28/Delitos_inform%C3%A1ticos.pdf* (Consultado: el 6 de noviembre de 2012)

CIBERDELINCUENCIA ORG, “Organizaciones Internacionales”, en *http://ciberdelincuencia.org/fuentes/organizaciones.php* (Consultado: 4 de julio de 2014)

CONCIL OF EUROPE, en *http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG* (Consultado: 4 de julio de 2014)

------, “Convenio Sobre la Ciberdelincuencia”, en *http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS_185_spanish.PDF* (Consultado: 18 de febrero de 2013)

------, “Informe explicativo, en *http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS%20185%20Explanatory%20report_Spanish.pdf* (Consultado: 18 de febrero de 2013)

CYBERCRIMENLAW, “The History of Global Harmonization on Cybercrime Legislation The Road to Geneva”, en *http://www.cybercrimelaw.net/documents/cybercrime_history.pdf* (Consultado: 18 de septiembre de 2014)

DIARIO OFICIAL DE LA FEDERACIÓN, “Decreto por el que se reforma, adiciona y deroga diversas disposiciones del Reglamento de la Ley Orgánica de la Procuraduría General de la República”, en *http://dof.gob.mx/nota_detalle.php?codigo=757798&fecha=01/11/2001* (Consultado: 19 de octubre de 2014)

EXCELSIOR ESPECIALES, en *http://www.excelsior.com.mx/nacional/2014/05/14/959260#imagen-1.* (Consultado: 7 de octubre de 2014)

GOBIERNO DEL ESTADO DE JALISCO, FISCALÍA GENRAL DEL ESTADO, en *http://fge.jalisco.gob.mx/policia-cibernetica* (Consultado: 24 de julio de 2014)

INTERPOL, “Redes I-24x7” en *http://www.interpol.int/es/INTERPOL-expertise/Data-exchange/I-24-7* (Consultado: 7 de octubre de 2014)

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS, “Delitos informáticos: generalidades”, en *http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf* (Consultado: 14 de Febrero de 2013)

POLICÍA DE SEGURIDAD PÚBLICA DISTRITO FEDERAL, en: *http://www.ssp.df.gob.mx/Pages/Ciberdelincuencia.aspx* (Consultado: 24 de julio de 2014)

REVISTA PROCESO DIGITAL, en *http://www.proceso.com.mx/?p=339886* (Consultado: 7 de octubre de 2014)

SEMANARIO JUDICIAL DE LA FEDERACIÓN, en *http://sjf.scjn.gob.mx/sjfsist/Paginas/tesis.aspx* (Consultado: 15 de octubre de 2014)

SISTEMA DE INFORMACIÓN LEGISLATIVA, en *http://sil.gobernacion.gob.mx/Reportes/Sesion/ReporteSesion.php?CveSesion=304264&Origen=BS&Camara=2* (Consultado: 12 enero de 2013)