Universidad Nacional Autónoma de Nicaragua-León

UNAN-León

Facultad de Ciencias Jurídicas y Sociales

Carrera de Derecho

Monografía para optar al título de Licenciado en Derecho

"LA CRIMINOLOGÍA COMO ELEMENTO CLAVE PARA LA REESTRUCTURACIÓN DEL ACTUAL SISTEMA DE CONTROL SOCIAL PENAL EN MATERIA DE CIBERDELINCUENCIA EN NICARAGUA"

Autores:

Br. Kasandra de los Ángeles Centeno Blessing

Br. Arleen Michelle Martínez Izaguirre

Tutor:

M. Sc. Juan Pablo Medina Rojas

León, 23 de septiembre de 2022

¡A la libertad por la Universidad!

RESUMEN.

Este estudio se intitula: **“La criminología como elemento clave para la reestructuración del actual sistema de control social penal en materia de ciberdelincuencia en Nicaragua”**; porque emerge substancialmente del análisis e interpretación del marco normativo regulatorio de la ciberdelincuencia en Nicaragua y la innegable pertinencia de la criminología para el fortalecimiento de la eficacia del control social penal y las políticas preventivas, necesarias para el adecuado tratamiento de un fenómeno criminal tan complejo como es la ciberdelincuencia. Consistiendo ésta en una investigación Dogmático-Jurídica, con enfoque cualitativo, en la que se ha empleado como fuentes de información fundamentalmente las leyes nacionales, algunas leyes extranjeras y la doctrina. Configurándose a lo largo de cuatro acápites que comprenden: primero las bases fundamentales en que se justifica el enfoque de esta investigación, donde se exponen los conceptos de Ciberdelincuencia, Criminología, Política Criminal y Control Social; segundo los parámetros en que se cimienta la eficacia normativa y su relación con la criminología, en el marco del control social penal en materia de ciberdelincuencia, exponiéndose nociones generales, requisitos elementales y pautas de evaluación que servirán de fundamento para el resto del estudio; tercero el análisis del régimen legislativo, nacional e internacional, adoptado por Nicaragua en materia de ciberdelincuencia, complementado con un estudio comparativo de la regulación Costarricense y Salvadoreña, que permita la valoración de los paramentos identificados en el capítulo anterior, exceptuándose aquellos que requieran de estudios prácticos; cuarto el análisis de la gestión político criminal en materia de ciberdelincuencia en Nicaragua, tomando como ejes de actuación los conocimientos brindados por la criminología; para así finalizar con la exposición de nuestras conclusiones generales y recomendaciones. En pertinencia con las líneas de investigación de la Facultad de Ciencias Jurídicas y Sociales proyectadas para el área general de Estado de Derecho, Gobernabilidad y Democracia, y el área específica de Ciencias Penales y Criminológicas; con los ODS 9, 16 y 17 de la agenda 2030, referentes a: Industria, innovación e infraestructuras; paz, justicia e instituciones sólidas; y alianzas para lograr los objetivos; y con los pilares de Integración Centroamericana y del Caribe referentes a: Seguridad democrática; y fortalecimiento de la institucionalidad regional.

León, 15 de agosto del 2022.

Msc. Edgard Blanco Guido
Jefe de departamento de Derecho público
Facultad de CC.JJ.SS. UNAN-León.
S. D.

Estimado maestro Blanco:

Me dirijo a usted deseándole continúe desempeñando con éxito el ejercicio de sus funciones.

El motivo de la presente misiva es para hacer de su conocimiento mi aprobación oficial del informe final de la investigación monográfica intitulada: **"LA CRIMINOLOGÍA COMO ELEMENTO CLAVE PARA LA REESTRUCTURACIÓN DEL ACTUAL SISTEMA DE CONTROL SOCIAL PENAL EN MATERIA DE CIBERDELINCUENCIA EN NICARAGUA",** elaborado por los bachilleres: **Kasandra de los Ángeles Centeno Blessing y Arleen Michelle Martínez Izaguirre** , ambas de los cursos regulares de la carrera de Derecho a quienes previamente usted me asigno como tutor para su investigación. Esta investigación cumple con los requisitos tanto formales como sustantivos para ser sustentada de conformidad con los artículos 41 al 79 del nuevo reglamento de formas de culminación de estudios de la UNAN-León.

Los sustentantes están aptos para realizar la lectura en acto formal de defensa oral del trabajo ante el tribunal examinador que usted designe.

Sin más a que referirme, me despido cordialmente de usted.

Prof. Msc. Juan Pablo Medina Rojas
Académico del departamento de Derecho público

AGRADECIMIENTOS.

Desde muy pequeños se nos ha inculcado el hábito de gratitud como sinónimo de emociones positivas, detrás de la cual yace el aprecio por las dádivas recibidas; sin embargo, es en base a la experiencia que reconocemos complejidad de ser agradecidos, a pesar que este sentimiento emana casi naturalmente. Por lo, en las limitadas líneas siguientes, trataremos de expresar integrantemente nuestros más sinceros agradecimientos:

Agradeciendo ante todo a Dios, como mandatan sus preceptos en Colosenses 3:17, porque él nos ha dado la fuerza y sabiduría, para cumplir con nuestros objetivos; por guiarnos a lo largo de todo este camino, darnos la paciencia suficiente y permitirnos seguir vivas hasta este momento, para poder ver los frutos de todos nuestros esfuerzos.

Y obviamente, a nuestra familia, por el apoyo incondicional, en todo momento de nuestro desarrollo, dándonos la oportunidad de una excelente educación en el transcurso de nuestra vida, sin medir los sacrificios para nuestro perfeccionamiento continuo; agradeciéndoles así mismo por todos los buenos valores que nos han inculcado, por el cariño, los cuidados y sobre todo por darnos un excelente ejemplo de vida.

Agradeciéndole especialmente a nuestro tutor, el M. Sc. Juan Pablo Medina, por la dirección y apoyo brindada para el desarrollo de la presente investigación, por el respeto a nuestras sugerencias e ideas y por la dirección y rigor con que ha facilitado a las mismas; por la confianza ofrecida desde el primer día; por la revisión cuidadosa que ha realizado de este texto y sus valiosas sugerencias en momentos de dudas.

Y reconociendo la ayuda recibida por otros docentes de la Facultad de Derecho, quienes sin ser nuestros tutores nos asistieron y auxiliaron en múltiples etapas de este proceso, orientando y atendiendo nuestras consultas, facilitándonos material bibliográfico y sugerencias, siempre bien recibidas.

Agradeciendo a nuestras amistades por el apoyo personal y humano, quienes sin ser conocedores de la materia nos brindaron tiempo de escucha, animándonos siempre a crecer como personas y como profesionales.

Y, por último, aunque te sorprenda, ahí va nuestro agradecimiento a ti, que nos estás leyendo ahora y participando de nuestro pensamiento.

ÍNDICE.

INTRODUCCIÓN 1

OBJETIVOS DE INVESTIGACIÓN 4

CAPÍTULO I

FUNDAMENTO TEÓRICO SOBRE EL CONTROL SOCIAL DE LA CIBERCRIMINALIDAD

1. LA CIBERDELINCUENCIA..... 5

1.1. Evolución terminológica del cibercrimen. 6

1.2. Origen y evolución histórica del cibercrimen. 8

1.3. Concepto de cibercriminalidad, cibercrimen o ciberdelincuencia. 10

1.4. Características de la ciberdelincuencia. 12

1.5. Clasificación de ciberdelitos. 13

1.6. Perfiles de detección del cibercrimen. 33

1.6.1. Perfiles del ciberdelincuente en el ciberespacio. 34

1.6.2. Perfiles de la víctima en el ciberespacio..... 39

1.7. Surgimiento de las teorías criminológicas explicativas de la ciberdelincuencia: Consideraciones de Sergio Arroyo. 41

2. LA CRIMINOLOGÍA..... 44

2.1. Antecedentes históricos. 44

2.1.1. Fuentes históricas. 45

2.1.2. Fuentes reales..... 46

2.2. Nacimiento de la criminología como ciencia. 48

2.3. Concepto de ciencia criminológica. 50

2.4. Características de la criminología..... 51

2.5. Objeto de estudio de la criminología. 51

2.6. Ampliación del objeto de estudio de la criminología. 52

3. EL CONTROL SOCIAL. 53
3.1. Origen de la categoría de control social. 53
3.2. Concepto de control social. 54
3.3. Características del control social. 56
3.4. Formas organizativas de control social. 57
3.4.1. Control social formal. 57
3.4.2. Control social informal. 58
3.5. Agencias de control social. 58
3.5.1. Agencias formales de control social. 59
3.5.2. Agencias informales de control social. 59
3.6. Control Social Penal. 59
3.7. El control social desde la moderna criminología. 61
4. POLÍTICA CRIMINAL. 62
4.1. Aspectos generales de la política criminal. 62
4.1.1. Desarrollo histórico de la política criminal. 63
4.1.2. Definición de política criminal. 65
4.1.3. Características de la política criminal. 66
4.1.4. Objetivo y área de investigación de la política criminal. 67
5. Recapitulación. 69

CAPÍTULO II

INCIDENCIA DE LA CRIMINOLOGÍA EN LA BÚSQUEDA DE LA EFICACIA NORMATIVA

1. Eficacia de las normas jurídicas. 71
1.1. Eficacia instrumental. 72
1.1.1. Condiciones de eficacia instrumental normativa que tienen su fundamento en la criminología. 73

1.1.1.1. La sociabilidad. 73
1.1.1.2. El conocimiento de las normas jurídicas. 75
1.1.1.3. Aceptación de las normas jurídicas. 77
1.1.1.4. La motivación de las normas jurídicas. 78
1.1.1.5. La aplicación de una adecuada técnica legislativa. 81
1.1.1.6. Otras condiciones de eficacia específicas para la materia ciberdelictual.83
2. Evaluación de los factores que afectan la eficacia de las normas jurídicas: 83
2.1. Proceso de evaluación legislativa:..... 83
2.2. Algunas pautas metodológicas dadas por la criminología para la evaluación legislativa..... 92
3. Recapitulación. 94

CAPÍTULO III

RÉGIMEN LEGISLATIVO ADOPTADO POR NICARAGUA, COSTA RICA Y EL SALVADOR EN MATERIA DE CIBERDELINCUENCIA

1. Regulación jurídica nacional..... 96
1.1. Nicaragua. 96
1.1.1. Constitución Política. 96
1.1.2. Código Penal. 97
1.1.3. Ley 1042, ley especial de ciberdelitos. 98
1.1.4. Ley 983, ley de justicia constitucional, énfasis en el recurso de Habeas Data……..100
1.1.6. Ley 621, Ley de Acceso a la Información Pública. 105
1.1.7. Código Procesal Penal. 107
1.2. Costa Rica. 110
1.2.1. Constitución Política. 110

1.2.2. Código Penal. 112

1.2.3. Ley N. ° 8968, de Protección de la Persona frente al Tratamiento de sus Datos Personales. 114

1.2.4. Código Procesal Penal. 115

1.3.1. Constitución Política. 118

1.3.2. Código Penal. 119

1.3.3. Decreto No. 260, Ley especial contra los delitos informáticos y conexos. 120

1.3.4. Decreto No. 551, Ley especial para sancionar infracciones aduaneras, énfasis en delitos informáticos. 121

1.3.5. Decreto No. 108, Ley contra actos de terrorismo, énfasis en delitos informáticos. 123

1.3.6. Código Procesal Penal. 124

2. Análisis comparativo del régimen legislativo nicaragüense. 138

3. Regulación Jurídica internacional. 147

3.1. Convenio Iberoamericano de cooperación sobre investigación, aseguramiento y obtención de prueba en materia de ciberdelincuencia. (Nicaragua)……...147

3.2. Tratado de asistencia legal mutua en asuntos penales entre las repúblicas de El Salvador, Guatemala, Honduras, Nicaragua, Costa Rica y Panamá. (Nicaragua, El Salvador, Costa Rica). 148

3.3. Convención Interamericana sobre asistencia mutua en materia penal. (Nicaragua, El Salvador, Costa Rica). 150

3.4. Convención de las Naciones Unidas contra la delincuencia organizada Transnacional. (Nicaragua, El Salvador). 151

3.5. Convenio de Budapest. (Costa Rica). 155

4. La cooperación internacional en materia de ciberdelincuencia. 161

4.1. La cooperación internacional y su arquitectura. 161

4.2. La cooperación judicial internacional en materia penal. 163

4.2.1. Algunas dificultades que afectan la cooperación internacional judicial en materia ciberdelictual. 163

4.2.2. Algunas pautas de utilidad para una satisfactoria cooperación internacional en materia ciberdelictual: 166

4.2.3. La cooperación internacional en materia de ciberdelincuencia en el contexto nicaragüense. 171

4.2.3.1. Observaciones sobre la cooperación internacional en Nicaragua en materia de cibercriminalidad..... 175

5. Recapitulación. 177

CAPÍTULO IV

GESTIÓN DE LA POLÍTICA CRIMINAL EN NICARAGUA

1. Relación interactual entre la política criminal y la criminología..... 179

2. Problemáticas actuales de la política criminal según Claus Roxin. 180

2.1. Primera Tesis: Las penas no son de ninguna manera un medio adecuado para la lucha contra la criminalidad. 180

2.2. Segunda Tesis: Las penas privativas de libertad son además un medio particularmente problemático en la lucha contra la criminalidad. 181

2.3. Tercera Tesis: La prevención es más efectiva que la pena. 182

2.4. Cuarta tesis: El sistema de reacción penal se debe ampliar y, sobre todo, complementarlo con sanciones penales similares de carácter social constructivo……..184

3. Algunos presupuestos para una adecuada política criminal. 186

4. Apreciación de la realidad Político Criminal Nicaragüense en materia de ciberdelincuencia..... 194

5. Recapitulación. 196

DISEÑO METODOLÓGICO: 198

CONCLUSIONES GENERALES. 199

RECOMENDACIONES. 201

FUENTES DE LA INFORMACIÓN. 203

ANEXOS: 218

INTRODUCCIÓN.

Indudablemente el desarrollo de las tecnologías de la información y la comunicación (más adelante TIC o TICs) ha traído consigo la evolución de la vida misma, trasmutando las principales actividades cotidianas de los particulares al espacio online para su facilitación e interconectándonos con el planeta entero sin mucha seguridad; cuestión que deja en evidencia la existencia de un nuevo aspecto social merecedor de custodia y del implemento de un marco normativo para la eficiente prevención del cibercriminen por constituir este un fenómeno criminal de complejo entramado.[1]

Todo esto considerando que la Ciberdelincuencia es un mal que se acrecienta significativamente sin limitación alguna, presuponiendo un peligro muy real para el mundo, el cual se adapta con mayor destreza en paridad con nuestros sistemas de justicia aprovechándose de las beneficencias de las TIC y la globalización para la comisión de actos reprochables.

Situación que ha dado lugar a la promulgación de instrumentos internaciones de cooperación internacional y la construcción y asentimiento de leyes especiales en la materia, dado precisamente las características propias del cibercrimen. Aprobándose, en ese mismo orden, por el Estado de Nicaragua la Ley No. 1042 “Ley Especial de Ciberdelitos”, publicada en la Gaceta – Diario Oficial No. 201 del 30 de octubre de 2020. [2]

Por consiguiente, la problemática que motiva esta investigación estriba de los limitados estudios existentes en dicha materia debido a su novicidad; necesarios para el planteamiento de un criterio apto sobre la regulación de la ciberdelincuencia en Nicaragua con relación a las ciencias criminológicas como clave para el

1. MIRÓ, Fernando. El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio [En línea]. Madrid: Marcial Pons, 2012. pp.13-30. [Consultado el 11 de abril de 2022]. Disponible en: https://www.marcialpons.es/media/pdf/9788415664185.pdf

2. QUEZADA, Martha. Análisis jurídico de la ley 1042: “Ley especial de ciberdelitos” [En línea]. Nicaragua: Poder Judicial, 2021, pp. 3-4. [Consultado el 10 de junio de 2022]. Disponible en:https://www.poderjudicial.gob.ni/iaej/pdf/Reformas/ANALISIS%20JURIDICO%20LEY%201042.%20LEY%20ESPECIAL%20DE%20CIBERDELITOS.pdf

aseguramiento del control social. Contando únicamente con la Ley Nº. 1042 “Ley Especial de Ciberdelitos” como paradigma de lo que nuestra política criminal supone, lo que obliga a la revisión y utilización de normas supletorias y rebuscadas doctrinas.

A razón de todo lo ya descrito surgieron las subsiguientes preguntas de investigación a las cuales se dará respuesta en el desarrollo de esta investigación:¿Qué planteamientos pueden proponerse para asegurar la eficacia del control social penal en Nicaragua en materia de cibercriminalidad?; ¿Cuáles son los beneficios que se obtendría de la aplicación de la criminología en el estudio del control social penal en Nicaragua en materia de cibercriminalidad?; ¿Qué tipo de política criminal adopta Nicaragua y como se ve reflejada o materializada en nuestro país?; ¿Qué dificultades normativas presenta la regulación del fenómeno de ciberdelincuencia en la Ley No. 1042?

Ahora bien, la importancia y vigencia de nuestra investigación se justifica en el creciente interés por comprender la funcionalidad y eficiencia del ordenamiento jurídico en materia de ciberdelincuencia, por ser la ciberdelincuencia una temática de preocupación mundial a la que la realidad nicaragüense no escapa. Así como en la escasez de recursos bibliográficos en nuestra alma mater referentes a la regularización jurídica ciberdelincuencial, sin abstraerse en el tratamiento de un delito en específico, lo que acrecienta nuestro interés por analizar e interpretar el marco normativo regulatorio de la ciberdelincuencia en Nicaragua, a fin de proporcionar comentarios fructíferos que nos permitan actualizar dichos recursos.

Considerando para ello a la criminología, con énfasis en el control social penal, como pieza elemental para la correcta regulación jurídica de la ciberdelincuencia, por ser esta una disciplina auxiliar del derecho penal, capaz de brindar respuestas especializadas al fenómeno ciberdelincuencial a través de herramientas conceptuales y metodológicas orientadas a la prevención y la persecución de los ciberdelitos.

Configurándose esta investigación a lo largo de cuatro acápites que comprenden: primero, las bases fundamentales en que se justifica el enfoque de esta

investigación, donde se exponen los conceptos de Ciberdelincuencia, Criminología, Política Criminal y Control Social; segundo, los parámetros en que se cimienta la eficacia normativa y su relación con la criminología, en el marco del control social penal en materia de ciberdelincuencia, exponiéndose nociones generales, requisitos elementales y pautas de evaluación que servirán de fundamento para el resto del estudio; tercero, el análisis del régimen legislativo, nacional e internacional, adoptado por Nicaragua en materia de ciberdelincuencia, complementado con un estudio comparativo de la regulación Costarricense y Salvadoreña, que permita la valoración de los paramentos identificados en el capítulo anterior, exceptuándose aquellos que requieran de estudios prácticos; cuarto, el análisis de la gestión político criminal en materia de ciberdelincuencia en Nicaragua, tomando como ejes de actuación los conocimientos brindados por la criminología; para así finalizar con la exposición de nuestras conclusiones generales y recomendaciones.

Por último, esta investigación está en correspondencia con a las líneas de investigación de la Facultad de Ciencias Jurídicas y Sociales proyectadas para el área general de Estado de Derecho, Gobernabilidad y Democracia, y el área específica de Ciencias Penales y Criminológicas; así como con los ODS 9: Industria, innovación e infraestructuras referente al apoyo del desarrollo de las tecnologías de la información en los países en desarrollo, garantizando un entorno normativo; ODS 16 y 17: Paz, justicia e instituciones sólidas y alianzas para lograr los objetivos que referencian la necesidad de crear instituciones eficaces y transparentes que rindan cuenta sobre sus acciones y que sean capaces de atender aquellas practicas reñidas con la ley; y también con los pilares de Integración Centroamericana y del Caribe referentes a: Seguridad democrática; y fortalecimiento de la institucionalidad regional.

OBJETIVOS DE INVESTIGACIÓN.

OBJETIVO GENERAL:

Formular criterios de orientación que contribuyan al fortalecimiento del actual sistema de control social penal en Nicaragua en materia de ciberdelincuencia conforme a la ciencia criminológica.

OBJETIVOS ESPECÍFICOS:

- Explicar las pautas metodológicas que ofrece la ciencia criminológica para la evaluación del impacto y funcionalidad de las leyes y la incidencia de estas en el tratamiento de la ciberdelincuencia.
- Analizar el marco legislativo nicaragüense en materia de ciberdelincuencia y su desarrollo en la gestión de la cooperación internacional.
- Identificar los principales inconvenientes político-criminales en materia de ciberdelincuencia en Nicaragua y proponer mejoras adaptadas a la realidad criminal de nuestro país.

CAPÍTULO I.

FUNDAMENTO TEÓRICO SOBRE EL CONTROL SOCIAL DE LA CIBERCRIMINALIDAD.

1. LA CIBERDELINCUENCIA.

La ciberdelincuencia comprende un acto delictivo, sin barrera física o geográfica que le limite, con mayor agilidad, mediante el empleo de las tecnologías de la información y la comunicación (TIC); diferenciado entre delitos dependientes de los medios informáticos (dependientes del uso de computadoras u otras formas de TIC) y delitos propiciados por los medios informáticos (delitos comunes facilitados por internet y tecnologías digitales).

Proviniendo su principal diferencia del papel que juegan las TIC en la comisión del delito, siendo esta su modus operandi, por lo que podrá afectar de forma negativa la confidencialidad, integridad o accesibilidad de los sistemas y datos informáticos o entrañar en si un delito común favorecido por el internet o las tecnologías digitales.[3]

Por lo que, al centrarnos en el estudio de la revolución de las TIC, como un concepto amplio, abierto y dinámico, conexo a todos los elementos y sistemas empleados para el tratamiento de la información, su intercambio y comunicación en la sociedad, podemos prever la importancia relacional que guarda el uso del ciberespacio con los extensos patrones de la vida diaria. Dado que la creación del ciberespacio ha modificado las relaciones económicas, políticas y sociales, pero, sobre todo, las personales, con los sistemas informáticos como forma de trabajo y diversión, las redes sociales, las redes de telefonía móvil totalmente conectadas, etc.

Indicando todo esto que la incidencia del ciberespacio en todos los aspectos de la vida diaria seguirá expandiéndose y evolucionando, y con ello el fenómeno

3. UNODC. La ciberdelincuencia, en resumen. [En línea] [Consultado el 11 de marzo de 2022]. Disponible en: https://www.unodc.org/e4j/es/cybercrime/module-1/key-issues/cybercrime-in-brief.html

cibercriminal, como evidencia de los efectos sociales que han acompañado la revolución de las TIC, dejando cada vez más en evidencia un nuevo aspecto social digno de protección y la necesidad de prevención del cibercrimen. [4]

Por lo tanto, en los siguientes apartados, nos enfocaremos en detallar el fenómeno cibercriminal, desde la visión fenomenológica y criminológica de la ciberdelincuencia.

1.1. Evolución terminológica del cibercrimen.

Tanto en la Doctrina Penal Alemana como Española, durante los años setenta, ochenta, noventa e inclusive a principios del siglo XXI, se empleó el término de delitos informáticos como referente a aquellos delitos tradicionales que recaían sobre bienes que representaban una configuración especifica en la actividad informática o nuevos objetos como el hardware y el software; centrándose únicamente en el medio utilizado y el objeto sobre el que ha de recaer el ataque como caracterización de los delitos informáticos, sin definir un bien jurídico protegido común a todos ellos, enfatizando en el ámbito de riesgo.

Por lo que los efectos sociales que trajo consigo la expansión de la tecnología informática, común a muchos bienes jurídicos, conllevo al legislador a precisar de la modificación de los tipos penales existentes o de la creación de distintos tipos que garantizaran una respuesta de protección eficaz al riesgo de la actividad informática. Considerándose además su posible incardinación a los tipos penales tradicionales o la reforma de los mismos, e incluso la creación de nuevos tipos, para una mejor protección. [5]

Sustituyéndose con el tiempo la denominación de delitos informáticos, ya hace más de treinta años, por la de cibercrimen y cibercriminalidad, en referencia al término

4. MIRÓ, Fernando. El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio [En línea]. Madrid: Marcial Pons, 2012. pp.13-30. [Consultado el 11 de abril de 2022]. Disponible en: https://www.marcialpons.es/media/pdf/9788415664185.pdf

5. Ibídem. pp. 25-36.

anglosajón *cybercrime*, procedente de la unión entre el prefijo *cyber*, derivado del término *cyberspace*, como parte integrante de los términos relacionados con las computadoras, ordenadores, realidad virtual…[6] y el término *crime*, como concepto que sirve para englobar la delincuencia en el ciberespacio.

Comprendiéndose delincuencia, con un significado más profundo conforme las ciencias jurídicas, como ya lo habrá explicado Ossorio, en las teorías penalistas, en correspondencia a un verdadero fenómeno social que no solo la ley pretende regular; refiriéndose a su vez a verdaderas conductas antisociales que requieren de su prevención y represión mediante las leyes penales. [7]

Cabe aclarar que aunque Internet constituye en sí mismo un medio informático, a través del cual se cometen las mayorías de las contravenciones, y se podría considerar que ciberdelitos entran dentro de la categoría de delitos informáticos, sin embargo, el concepto de cibercriminalidad esclarece que sus implicaciones de riesgo van mucho más allá de la utilización de TIC y se relaciona más con el hecho de que estos comportamientos están unidos, actualmente, a redes telemáticas, con las problemáticas político-criminales que ello plantea, amplificando así el catálogo de infracciones del cibercrimen, terminando la cibercriminalidad abarcando la criminalidad informática.

Ya que el término cibercrimen logra englobar todas las tipologías de comportamientos que deben estar previstas en la unión de Internet y las TIC como medio de comisión delictiva, alcanzando además la más propia categorización del tipo. [8]

---

6. Diccionario de la lengua española, Real Academia Española. Ciber. [En línea] [Consultado el 11 de marzo de 2022]. Disponible en: https://dle.rae.es/ciber-

7. OSSORIO, Manuel. Diccionario de Ciencias Jurídicas, Políticas y Sociales [En línea]. Guatemala: Datascan, S.A, 2018 [Consultado el 11 de marzo de 2022]. Disponible en: https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnxjb25zdWx0b3Jlc2xlZ2FsZXNkZWxub3Jlc3RlfGd4OjVjMTM0NzQ5MWYyMmIyMDE

8. MIRÓ, Fernando. Op. Cit. pp. 36-39.

1.2. Origen y evolución histórica del cibercrimen.

Es innegable que la aparición de internet y los sistemas informáticos marcaron un hito para la historia de la humanidad, modificando así el acceso a los sistemas de información y evidenciando cada vez más claramente la fragilidad de la seguridad existente en torno a estos nuevos paradigmas y herramientas cibernéticas.

Siendo así como algunos lograron aprovecharse del nacimiento del internet en 1969, adaptándose con mayor facilidad a los cambios que trajo consigo un mundo globalizado, desarrollando técnicas y métodos que quebrantaron los inmaduros sistemas de seguridad de aquel entonces, tomando ventaja sobre las autoridades y su escasa preparación para abordar este nuevo problema. [9]

Por lo que en la búsqueda del origen del cibercrimen la historia nos remite a principios de la década de 1970, donde un pequeño e inofensivo silbato azul causo un significativo impacto en el sistema telefónico de Estados Unidos, el cual sobre la base de un tono puro de 2600Hz, casualmente coincidente con el tono emitido por la telefonía, permitió a un joven ingeniero llamado John Draper realizar llamadas de larga distancia de forma gratuita, quien utilizando está idea, construyó un dispositivo llamado “Blue Box” capaz de reproducir diferentes tonos reconocidos por el sistema telefónico de forma que le permitiera modificar y controlar el comportamiento de este a su propio beneficio; dando las noticias de su existencia la vuelta al mundo, incrementando el movimiento “Phreakers’, donde hasta figuras de renombre en la actualidad, como Steve Woznkiak y Steve Jobs tuvieron presencia.

No obstante, aún no existía ningún ciberdelito real, hasta que, en la década de 1980, una persona hackeó la computadora de otra para manipular datos e información personal. Siendo esta la primera persona en ser declarada culpable de un delito cibernético, en el año 1981, Ian Murphy, también conocido como Capitán Zap, quien había pirateado la compañía telefónica estadounidense para manipular su reloj

9. OGDI. Historia del Cibercrimen. [En línea] [Consultado el 03 de marzo de 2022]. Disponible en: https://ogdi.org/historia-del-cibercrimen

interno, permitiéndoles a sus usuarios realizar llamadas gratuitas. Y aunque las empresas telefónicas fueron el primer objetivo, los bancos, las tiendas web e incluso los particulares siguieron rápidamente su ejemplo. [10]

Y si bien, el protagonismo inicial de esta historia lo tuvieron las terminales informáticas y la información personal en ellas contenidas, tras la aparición de nuevas formas de afectar a la intimidad de las personas, por adquirir dichas las terminales informáticas y la información adjunta un valor económico y servir para la realización de transacciones, conllevaron consecuentemente a nuevas formas de criminalidad económica relacionadas con los ordenadores y muy especialmente el fraude informático, que evoluciono hacia el *scam*, el *phishing* y el *pharming* cuando apareció internet; y así finalmente, con la evolución del ciberespacio comenzaron a surgir nuevas formas de criminalidad que aprovechaban la trasnacionalidad de internet para atacar intereses patrimoniales y personales de usuarios concretos, además de afectar a intereses colectivos por medio del ciberracismo, ciberterrorismo, etc. Y así, hasta nuestros días donde han aparecido nuevas formas de delincuencias en relación con los nuevos servicios y usos del entorno digital.

Y es así, como se logra evidenciar como la aparición de Internet marca un antes y un después como forma de división, criminológica, entre la criminalidad informática y la cibercriminalidad, terminando esta última por abarcar la primera; distinguiéndose así la primera generación de la cibercriminalidad por el empleo de ordenadores para la comisión de delitos, hasta transfigurarse en una segunda generación caracterizada por la comisión de delitos a través de internet, y así, hasta reconocer una tercera en la que los delitos están absolutamente determinados por el uso de Internet y las TIC.

10. PASCUAL, Ivan. *Ciberdelincuencia. Desarrollo y persecución tecnológica* [En línea]. Tesis de titulación en Telemática. Universidad Politécnica de Madrid, 2013, pp.88-96 [Consultado el 03 de marzo de 2022]. Disponible en:https://www.google.com/search?q=PASCUAL%2C+Ivan.+Ciberdelincuencia.+Desarrollo+y+persecuci%C3%B3n+tecnol%C3%B3gica&oq=PASCUAL%2C+Ivan.+Ciberdelincuencia.+Desarrollo+y+persecuci%C3%B3n+tecnol%C3%B3gica&aqs=chrome..69i57.4427820j0j7&sourceid=chrome&ie=UTF-8#

Incidiendo esto directamente en el ámbito legal, tras marcar un nuevo siglo donde la preocupación ya no está solo dirigida a la información que pudieran contener los sistemas informáticos y la afectación a la intimidad o el patrimonio, sino en el ciberespacio, que muestra un nuevo aspecto social digno de protección, donde se podrían afectar otros nuevos bienes jurídicos como la intimidad sexual, la dignidad o la propia seguridad nacional. [11]

1.3. Concepto de cibercriminalidad, cibercrimen o ciberdelincuencia.

Como a bien lo ha resaltado la Oficina de las Naciones Unidas contra la droga y el delito (UNODC) hasta el momento no contamos con definición alguna sobre ciberdelincuencia, que conste de aceptación a nivel universal. [12] Esto en gran parte se debe a la utilización, en el ámbito científico, de neologismos procedentes de la traducción al castellano de términos de otras lenguas, empleándose indiscriminadamente los términos cibercrimen, ciberdelito, cibercriminalidad y ciberdelincuencia en muchos casos como un sinónimo y en otros pretendiendo dotarles de sentidos distintos. [13]

Comprendiendo el término cibercrimen, sin escapar de su carácter polisémico, como un comportamiento concreto que reúne una serie de características criminológicas, y legales, relacionadas con el ciberespacio (en su sentido tipológico); y a su vez, también es empleado para la identificación de un tipo penal concreto con un presupuesto y una sanción, que pretende prevenir la realización de conductas, que afectan a bienes jurídicos dignos de protección, en el ciberespacio (en su sentido normativo).

11. MIRÓ, Fernando. El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio [En línea]. Madrid: Marcial Pons, 2012. pp. 27-39. [Consultado el 11 de abril de 2022]. Disponible en: https://www.marcialpons.es/media/pdf/9788415664185.pdf

12. UNODC. La ciberdelincuencia, en resumen. [En línea] [Consultado el 11 de marzo de 2022]. Disponible en: https://www.unodc.org/e4j/es/cybercrime/module-1/key-issues/cybercrime-in-brief.html

13. MIRÓ, Fernando. Op. Cit. pp.33-34.

Cabe destacar que el término cibercrimen guarda una relación directa, en su sentido tipológico, con el de cibercriminalidad; refiriéndose el término cibercriminalidad al fenómeno del crimen en el ciberespacio, y en muchos casos, el término cibercrimen para situar dentro de ese fenómeno a un tipo de comportamiento en concreto. No obstante, en ocasiones, el término cibercrimen, en concepción amplia, es utilizado para hacer referencia a todos los comportamientos que reúnen las características tipológicas que conforman el fenómeno cibercriminal, como un sinónimo de ciberdelincuencia.

Lo que nos permite apreciar, dentro del catálogo de definiciones ya existentes, una serie de elementos claves para la precisa determinación de dicho término; consistentes en un comportamiento delictivo realizado dentro de una nueva realidad, propiciada por el ciberespacio, mediante el empleo de las tecnologías de la información y la comunicación (TIC), donde podremos apreciar conductas cuyo contenido ilícito es nuevo y se relaciona directamente con los nuevos intereses o bienes sociales existentes en el ciberespacio (ataques tecnológicos, de datos, sistemas, redes), así como comportamientos tradicionalmente ilícitos propiciados por los medios informáticos. [14]

Siendo así como, en el Convenio Iberoamericano de cooperación sobre investigación, aseguramiento y obtención de prueba en materia de ciberdelincuencia, podemos apreciar en su art. 2 numeral 1, que dicho término se define como: “Cualquier forma de criminalidad ejecutada en el ámbito de interacción social definido por el uso de las tecnologías de la información y la comunicación”. [15]

14. MIRÓ, Fernando. Op. Cit. pp.39-44.

15. Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de prueba en materia de Ciberdelincuencia, hecho en Madrid, el día 28 de mayo de 2014. Aprobado por Nicaragua, a través del DECRETO A.N. No. 8651 del 25 de febrero de 2020, publicado en La Gaceta – Diario Oficial, No. 42, del 03 de marzo de 2020 y ratificado mediante DECRETO PRESIDENCIAL No. 08-2020 del 16 de abril de 2020, publicado en La Gaceta – Diario Oficial, No. 73 del 24 de abril de 2020.

Considerándose los delitos con mayor afluencia en internet aquellos que atentan contra la honra (injuria, calumnia y difamación), exhibición de imágenes de contenido sexual, divulgación de textos ofensivos y fraudes relacionados a lo económico (cuentas bancarias y tarjetas de crédito). [16]

Comprendiéndose por delitos cibernéticos, dentro de la legislación Nicaragüense, como lo estipula el art. 3, de la Ley No. 1042, Ley Especial de Ciberdelitos, en su numeral cuarto, cito: "Acciones u omisiones, típicas, antijurídicas, continuas o aisladas, de carácter penal, cometidas en contra de personas naturales y/o jurídicas, utilizando como método, como medio o como fin, los datos, sistemas informáticos, Tecnologías de la Información y la Comunicación y que tienen por objeto lesionar bienes jurídicos personales, patrimoniales o informáticos de la víctima". [17]

1.4. Características de la ciberdelincuencia.

El fenómeno ciberdelincuencial constituye una acción muy compleja, caracterizada principalmente por: El entorno en que se produce, la extraterritorialidad y universalidad, así como otros aspectos particulares correspondientes a dicha acción, al sujeto, el resultado, etc. Características que en lo siguiente procederemos a estudiar a detalle.

Resultando indispensable, antes de todo, destacar que esta clase de delitos abarcan una gran cantidad y variedad de acciones de distinta naturaleza, por lo que en su generalidad se caracterizan por ser:

- **Universales:** Pueden cometerse en cualquier parte del mundo; viéndose afectada la criminalidad física por el ciberespacio, que ha facilitado la ausencia

16. OLIVEIRA, Edmundo. "Globalización, red cibernética y delito por internet". En: "*Justicia penal, política criminal y Estado social de derecho en el siglo XXI"*. Coord. TIFFER, Carlos. Argentina: EDIAR, 2015, p. 253. ISBN: 978-950-574-329-2

17. Nicaragua. Ley No. 1042, "Ley Especial de Ciberdelitos". *La Gaceta – Diario Oficial*, del 30 de octubre de 2020, No. 201. Disponible en: http://legislacion.asamblea.gob.ni/normaweb.nsf/($All)/803E7C7FBCF44D7706258611007C6D87

del sujeto activo al momento de la consumación del hecho delictivo, pudiéndose encontrar en un país muy lejano al momento de cometer un delito, cuyos resultados son vistos en un país distinto y lejano o en muchos países al mismo tiempo.

- **Extraterritoriales:** Pueden ser cometidos y perseguidos tanto en el territorio nacional como internacional.
- **Instantáneos:** Son actos que pueden llevarse a cabo de forma rápida y sencilla; su consumación se agota en el mismo momento en que se han realizado todos los elementos de la descripción penal.
- **Procedentes del ciberespacio:** En un espacio virtual, que supone una nueva realidad, que permite al ser humano transcender a su realidad corpórea y física.
- **De carácter técnico:** Por lo que requieren del empleo de la informática y las tecnologías de la información y la comunicación para su comisión; razón por la cual presentan grandes dificultades para su comprobación.
- Además, cabe destacar, como característico de estos delitos, que facilitan la comisión del ilícito por los menores de edad.

1.5. Clasificación de ciberdelitos.[18]

Es innegable, y no está demás repetirlo, que el avance tecnológico y la globalización han transfigurado la vida diaria, admitiendo un nuevo campo de acción, no solo para la facilitación de las tareas rutinarias, sino también aprovechado por los delincuentes; generando nuevas modalidades de delitos y facilitando la comisión de delitos tradicionales, manifiestos en un catálogo muy amplio del cibercrimen, por lo que surgen clasificaciones muy diversas, caracterizando, de forma más limitada, sus similitudes, a fin de facilitar, a los investigadores, desarrolladores y creadores de la ley, su identificación.

En tal sentido, Miró, categoriza el cibercrimen desde una perspectiva más amplia, que engloba más que solo tipos penales, tomando en consideración tipologías de conductas peligrosas, para los bienes jurídicos esenciales, caracterizadas por el

18. MIRÓ, Fernando. Op. Cit. pp. 47-118

empleo de las TICs. Diferenciando tres tipos de cibercrímenes, que posteriormente distinguirá con otros tres, a razón de:

- La incidencia de las TICs en el comportamiento criminal;
- El propósito criminal con el que se actúa; y
- El contexto de incidencia del ciberespacio al que afectan los delitos.

Con el propósito de identificar los ámbitos principales que afecta el cibercrimen y, encontrar para cada categoría, por lo menos, un ámbito de referencia en la criminalidad común, que permita la comprensión del fenómeno y su mayor prevención.

Sistematizando el cibercrimen, en atención a los distintos intereses sociales con trascendencia jurídica que se pueden ver afectados, entre:

- **Cibercriminalidad económica:** Cuyo propósito radica en la obtención de un beneficio patrimonial por parte de quien realiza el delito.
- **Cibercriminalidad social:** Son aquellos que tienen que ver con las relaciones sociales entre las personas; No son más que la transposición al ciberespacio de los crímenes tradicionales derivados de conflictos entre personas.
- **Cibercriminalidad política o ideológica:** Referente a la acusación de daños a infraestructuras u objetos sensibles, con el propósito de desestabilizar a un Estado o una institución política.

Y distinguiendo el cibercrimen, fenomenológicamente, atendiendo la incidencia de las TICs en la esencia de la conducta criminal, en:

- **Ciberataques puros:** Posibles únicamente en el ciberespacio; constituyendo el empleo de las TICs el medio y el objeto de tales ataques, por lo que es imposible producir la esencia de ilicitud si no es en el ciberespacio.
- **Ciberataques replica:** Son el reflejo de las formas de conductas ilícitas tradicionalmente ejecutadas en el espacio físico, cuya presencia en el espacio virtual le hace parecer prácticamente nueva; pasando a ser la red el nuevo medio a través del cual se comete una infracción que utilizaba anteriormente de otros medios para llevarse a cabo.

- **Ciberataques de contenido:** Constituyen una forma concreta de los denominados ciberataques réplica, pero con una singularidad tal y con problemáticas jurídicas tan especiales que merece ser tratado por separado. Dicha categoría conglutina todas aquellas en las que el centro de la infracción lo constituye el contenido que se comunica o se transmite a través de las redes.

Para, a raíz de tales modalidades, partir hacia una clasificación más clara y detallada de las conductas antijurídicas, y sus subtipos, que comprenden el cibercrimen. Consistentes en:

- **Hacking o acceso ilícito a sistemas informáticos:** Referente a cualquier conducta por la cual un sujeto accede a un sistema o equipo informático sin autorización del titular, de forma tal, que podrá utilizar o acceder a cualquier tipo de información que esté en el sistema.

Cabe destacar que el *hacking*, en sentido estricto, se puede llevar a cabo de diversas formas, a través de la:

  - Búsqueda de vulnerabilidades en los sistemas informáticos derivadas de una deficiente programación.
  - Búsqueda de un cambio tecnológico que hace obsoleta la formulación binaria existente.
  - Búsqueda y uso de las puertas que involuntariamente el propio titular del sistema informático o cualquiera de los múltiples sujetos que interaccionan con él pueden haber dejado abiertas.

En todo caso, el *hacking* es siempre, por su propia naturaleza, un acceso remoto; realizado a distancia por el sujeto que, normalmente a través de Internet, se entromete en un sistema sin tener contacto físico con él. De esta manera, no es considerado como *hacking* el acceso directo, en la propia terminal, y no autorizado a un sistema informático.

- **Sabotaje cibernético e informático:**

El sabotaje informático, incluye en él, tanto:

- Los comportamientos ya conocidos y asumidos como comunes en el entorno virtual, consistentes en el envío a través de redes telemáticas de virus informáticos que aprovechan la inmensidad de la Red para multiplicarse y acceder a miles de terminales, y
- Cualesquiera otras formas de destrucción de archivos o datos de terminales concretos y determinados, con fines industriales o de daño individual.

El sabotaje cibernético puede afectar a:

- Los propios sistemas informáticos y demás elementos de hardware que lo conforman y que son evaluables económicamente.
- La información contenida en los citados sistemas y que puede tener un valor económico o personal, en el sentido sentimental y relacionado con su propia dignidad, para el sujeto pasivo.
- La propia funcionalidad del sistema informático en el marco de la actividad económica de que se trate.

Este tipo de actividades ilícitas preocupará cada vez más a la sociedad conforme se vayan trasladando al ciberespacio servicios públicos y privados que hasta el momento únicamente se ofrecían en el espacio físico.

- **Malware:** Forma más popular de sabotaje cibernético; ejecutada mediante la distribución de malware o software malicioso y la consecuente infección de virus destructivos destinados a dañar, controlar o modificar un sistema informático.

Cabe destacar que estos virus no solo han aumentado en cantidad con el transcurso de los años y con la popularización de la interconexión, sino que también han ido evolucionando y adaptándose a las nuevas necesidades.

Y Dentro del malware hay distintas modalidades de software con objetivos muy distintos tales como:

- Los que tratan de destruir el sistema o su información como los virus y algunos tipos de gusanos (*worms*) o troyanos (*trojans*).

- Los que permiten el acceso remoto del sistema informático a través de la Red como los *botnets* o los *rootkits* que esconden el software malicioso o permiten el control del sistema.
- Los *keystroke loggers* o *spyware* que capturan información de los sistemas informáticos.
- El denominado *adware*, menos nocivo que todos los anteriores, pero de algún modo también molesto, pues se trata de programas anexos que en realidad espían nuestros hábitos en Internet.

Ocasionando el menoscabo de archivos y datos que pueden tener, un valor sentimental o personal, no evaluable económicamente en el sentido de ser bienes insustituibles, o con un valor económico derivado del propio esfuerzo que ha supuesto su producción y del valor potencial que en sí misma tiene en el mercado.

- **Sabotaje de *insider*:** Alusivo a la conducta del *insider* o persona que trabaja (o trabajaba, pero aún tiene acceso a los sistemas) en la empresa o institución víctima, y aprovecha su posición para, como venganza o motivos similares, destruir la mayor cantidad posible de información a través de redes telemáticas.

- **Ataques DoS y DDoS:** Forma de ataque directo al sistema informático que, generalmente, se dirige hacia algunos prestadores de servicios en Internet, pero que puede afectar casi a cualquier sistema del ciberespacio.

Los *Denial of Services* o ataques de denegación de servicios (DoS), consistentes en la utilización de técnicas para cargar los recursos del ordenador objetivo y producir la negación de acceso del servidor a otros sistemas informáticos; tienen por finalidad:

- Dañar la reputación de las empresas que ofrecen servicios en Internet, impidiendo el correcto funcionamiento de sus actividades.
- Perjudicar a un competidor en algún tipo de servicio en Internet.
- *Hacktivismo* político, esto es, de difusión de mensajes de protesta en Internet generalmente dirigidos contra organismos o Estados que,

según las comunidades de usuarios de Internet, ponen en riesgo la idea del ciberespacio abierto que ellos defienden.

Empleando, dos métodos básicos, para producir el ataque; consistentes en:

- **La explotación de una vulnerabilidad descubierta en una máquina objetivo que constituye el denominado «ataque de vulnerabilidad»:** Se aprovecha algún tipo de fallo en la configuración del *software* o del recurso informático para enviar unos paquetes de datos que provocan un estado no previsto por el programador en el momento de su diseño que puede suponer la generación de un bucle infinito, o la ralentización de la velocidad de ejecución de la aplicación, etc., provocando el cese del funcionamiento del sistema o su inutilización total o parcial.
- **El envío hacia la víctima de un amplio número de mensajes de apariencia legítima, conocido como «ataque de inundación»:** Los mensajes producen el agotamiento de determinados recursos críticos para que los usuarios no puedan hacer uso de los mismos.

Cabe destacar, entre los bienes o intereses sociales dignos de protección que pueden ser afectados por este tipo de ataques, los siguientes:

- El patrimonio de los titulares de los sistemas informáticos o de los archivos contenidos en ellos
- El interés socioeconómico colectivo en que la actividad económica en internet sea segura, sin que la conexión de sistemas informáticos a la red pueda poner en riesgo los mismos o la información en ellos contenidos.
- La libre expresión en internet, al impedírseles a las víctimas el comunicar sus mensajes y llevar a cabo su actividad.
- Los derechos de todos los usuarios de internet al acceso a los servicios existentes en la red.

Por otro lado, las siglas DDoS correspondientes a *Distributed Denial of Services* o denegación de servicio distribuida. Estos ataques que vienen a ser una evidente

evolución del DoS, consisten en que, frente a la terminal única que realiza el ataque, son numerosas las máquinas que, de forma coordinada, atacan a una sola víctima.

- **Spam:** Consistente en el correo electrónico no solicitado que suele enviarse a numerosas direcciones a través de una dirección electrónica de las ofrecidas por los servicios de correo gratuitos estilo Hotmail, o desde un sistema informático infectado, convertido en *bot* e integrado en una *botnet* y utilizado por el *spammer*, que adquiere las direcciones de correo *hackeando* sistemas informáticos o utilizando *spyware* u otros sistemas de búsqueda de direcciones electrónicas a través de la Red. Lo cual supone el:
    - Envío ilícito de publicidad;
    - Intento de infección del sistema por medio de malware;
    - Intento de phishing; y
    - Tampoco debe despreciarse la enorme gravedad que supone el mero hecho de recibir correos indeseados aun en el caso de no ser infectado por ellos.

- **Ocupación o uso de redes sin autorización:** Considerados ataques directos a elementos de las TIC, los cuales se pueden llevar a cabo de:
    - **La utilización de una terminal de comunicación titularidad de otro sujeto:** En este caso el elemento afectado son las redes más que a las terminales, tales como redes de comunicación de televisión por cable o redes telemáticas.
    - **Comportamientos de piratería de señales de emisión radiofónica, televisiva y de Internet:** Los cuales mediante la creación de *software* específico que se instala en un sistema informático «piratean la señal digital de que se trate», o a través de otros sistemas más arcaicos como la duplicación de claves o similares. Los elementos afectados son los servicios, concretamente aquellos generales de comunicación y difusión de contenidos de telecomunicación.

- ***Antisocial networks*:** Consistente en la manipulación de redes sociales o de grupos de ellas con la finalidad de utilizarlas posteriormente para el fraude o para

cualquier otro tipo de ciberdelitos. De tal manera que no consiste en una conducta criminal sino más bien en un comportamiento preparatorio de las posteriores conductas criminales.

Y es que, en efecto, las redes sociales tienen algunas propiedades intrínsecas que las hacen ideales para ser aprovechadas por adversarios o por quienes quieren utilizarlas para defraudar a otros:

- Tienen una gran, y ampliamente distribuida, base de usuarios
- Está formada por grupos de usuarios que comparten similares intereses sociales lo cual conlleva un desarrollo de la confianza entre ellos y el uso de recursos compartidos
- La plataforma permite a los usuarios la instalación de aplicaciones pensadas contra el fraude y similares cibercrímenes.

- **Ciberfraudes:** Son aquellos en los que las redes telemáticas se convierten en el instrumento mediante el cual lograr un beneficio patrimonial derivado de un perjuicio patrimonial a una víctima. Así, algunas de las más conocidas son:
  - Fraudes de tarjetas de crédito;
  - Fraudes de cheques;
  - Estafas de inversión;
  - Estafas piramidales realizadas a través de internet;
  - Estafas de la lotería;
  - Ventas online defraudatorias en las que no se envía el producto comprado (o se envía con otras características, como en el *auction fraud*) o no se paga lo que se ha recibido o se cobran servicios no establecidos previamente;
  - Estafas de inversión en las que se cobran gastos no previstos o no se explican pérdidas inesperadas;
  - Ataques de *scam* en los que se prometen cantidades importantes de dinero a cambio de pequeñas transferencias relacionadas con ofertas de trabajo, loterías, premios u otros; y
  - Los denominados *auction fraud*, o fraudes en las subastas.

- **Ciberfraudes burdos o *scam*:** Se tratan de las tradicionales estafas en las que, en este caso, la forma de comunicación entre las personas para la realización del engaño es el Internet, ya sea por correo electrónico o mediante el uso de las redes sociales.

Se le suele denominar “burdos” debido a que el engaño es poco elaborado y el error de la víctima puede ir más allá de lo común. Incluyéndose en esta categoría:

  - Las denominadas «cartas nigerianas», estafa clásica.
  - El famoso «timo de la estampita» en el que el engaño se logra explotando el ánimo de lucro de la víctima.
  - Otras que han surgido posteriormente como la de la lotería, la del trabajo desde casa, etc.

Consistiendo el factor humano, en este tipo de estafas, en el elemento esencial para que el engaño tenga éxito. Pues lo que se busca es interesar a la víctima o ganarse su confianza para que sea ella quien finalmente realice el acto de disposición patrimonial que le perjudica.

- ***Phishing o pesca de incautos*:** Constituye la modalidad estrella dentro de las conductas de ciberfraudes. Mecanismo criminal que emplea ingeniería social y subterfugios técnicos para robar los datos de identidad personales de los consumidores y los de sus tarjetas de crédito o cuentas bancarias.

Estos ataques pueden manifestarse de dos formas básicas:

  - **A través del uso de la ingeniería social:** Se utiliza la identidad personal de otro (*spoofng*) mediante la falsificación de sitios web, para conducir a los consumidores a que confíen en la veracidad del mensaje y divulguen los datos objetivos.
  - **Utilizando otros artificios técnicos:** Redireccionar un nombre de dominio de una página web verdadera situada en la memoria caché del sujeto o de otro modo a una página web falsa, o monitorizar la intervención del sujeto en la verdadera; en estos casos se utiliza el término de *pharming*.

Incluyendo típicamente, para su comisión, tres componentes clave:

- **El mensaje:** Las potenciales víctimas reciben un reclamo a través de un medio electrónico. En la mayoría de las ocasiones se trata de un correo electrónico remitido por el delincuente, pero también puede ser un SMS, VoIP.
- **La interacción:** Recibido el mensaje por el usuario, a continuación, se requiere que la propia víctima acuda a la web que se ha construido de manera idéntica a la de una organización de confianza, como un banco o una popular web de subastas, que instale el malware o que remita la información sensible.
- **La utilización efectiva de la información robada:** En algunos casos el delincuente usa directamente los datos de la víctima suplantando su identidad; no obstante, normalmente el *phisher* no explota por sí mismo la información obtenida, sino que la vende a terceros. De este modo, se ha generado un mercado negro de compraventa de información robada.

Distinguiéndose entre las diferentes modalidades de phishing existentes el:

- **Phishing tradicional:** Utilización de imagen corporativa de entidades o instituciones solicitando datos bancarios indiscriminadamente.
- **Spear phishing:** Phishing dirigido a entidades bancarias u otro tipo de organizaciones concretas, no a objetivos indiscriminados.
- **Business Services phishing:** El objetivo buscado son los empleados de entidades que utilizan servicios de Internet.
- **Whaling:** Phishing dirigido a los directivos o individuos pertenecientes a los niveles altos de las organizaciones.
- **Vishing:** Esta práctica consiste en la utilización de mensajes de telefonía basada en voz sobre IP, para conseguir de la víctima información personal, financiera o cualquier otro tipo de datos confidenciales.
- **Phishing basado en malware:** Cualquier tipo de phishing en el que se hace uso de software malicioso en el ordenador del usuario.

E identificándose entre los métodos más comunes para garantizar su éxito:

- ***Man-in-the-middle:*** A través de esta técnica, el atacante es capaz de controlar y registrar las transacciones e información sensible del usuario, interponiendo un *proxy* entre el cliente y el servidor web. Para ello se emplean diferentes técnicas:
  - *Proxies* transparentes, que se sitúan en la misma red o ruta que el servidor real;
  - DNS Cache *Poisoning* (envenenamiento de caché de DNS), que permite el enrutamiento de IP falsas;
  - La ofuscación de URL, que permite redirigir el tráfico de datos a su servidor; o
  - Configurando el *proxy* en el navegador.
- **Cross-site scripting:** En este caso el engaño consiste en introducir código o URL falsas en una web real. De este modo la mayor parte del contenido web es original, sin embargo, una parte, la referida a la información sensible, está construida para obtener los datos objetivos sin que el usuario pueda detectar anomalías.

Esta técnica se centra en el aprovechamiento de vulnerabilidades que el cliente posibilita, lo que permite:

- Mediante el uso de *exploits,* falsear la dirección que aparece en el navegador.
- Aprovechar los fallos de aplicaciones java, que permiten embeber servidores remotos en la red local del usuario.
- Falsear las ventanas emergentes (*pop-ups*) abiertas desde una página web auténtica.
- Aprovechamiento de alguna vulnerabilidad de internet Explorer o del sistema operativo del cliente, permitiendo descargar troyanos de tipo *keylogger* que robarán información confidencial del usuario.

- ***Identity theft* y cibersuplantación de identidad o *spoofng*:** El robo de identidad podría definirse como la adquisición en todo o en parte por un sujeto de los datos de otro sujeto para su posterior uso como si le pertenecieran a él.

No obstante, cuando se habla de *identity theft* se suele utilizar presuponiendo el futuro uso delictivo de la suplantación, esto es, como la utilización o explicación de los datos de identificación personal u otro tipo de información de la persona como el nombre, el número de DNI, etc., para cometer fraude o participar en otras actividades ilegales.

Y no está demás mencionar que en el ciberespacio el robo de identidad resulta más sencillo de ejecutar y potencialmente mucho más peligroso por las siguientes razones:

- La eliminación de la inmediatez física y las posibilidades técnicas para la obtención de información personal y para la simulación, hacen que sea posible obtener datos privados necesarios para suplantar a la persona y actuar directamente haciéndose pasar por ella.
- Son múltiples las personas conectadas en el ciberespacio que realizan operaciones financieras y de cualquier otro tipo.

Empleando el robo de identidad generalmente como primer paso para la ejecución posterior de algún tipo de fraude informático, generalmente el *phishing.*

El robo de identidad en Internet se puede llevar a cabo de muchas formas, algunas veces a través de ingeniería social o por medio de ingeniería informática. En esta última modalidad se encuentra el denominado *spoofing,* de los cuales se diferencian al menos cinco formas:

- **IP *spoofng*:** En el que mediante la utilización de programas específicamente destinados a ello se sustituye la dirección IP original por otra.
- **ARP *spoofng*:** En el que se falsean las denominadas tablas ARP de una víctima para llevar a su sistema MAC a que envíe los paquetes al host atacante en vez de a su destino.

- **DNS *spoofng*:** En el que lo que se modifica es el nombre de dominio-IP de un servidor DNS, aprovechando alguna vulnerabilidad, lo cual se suele utilizar para el *pharming* en el que el sujeto pone la dirección web de una entidad bancaria oficial y se le remite a una web falsa.
- **Web *spoofng*:** Quizás el más común de todos estos ataques, en el que, a través de un enlace u otras formas de engaño, se hace pasar una página web, imitada y albergada en otro servidor, por la real, por medio de un código que solicita la información requerida por el sistema víctima a cada servidor original y remite a la web falsa.
- ***Mail spoofng*:** Consistente en la suplantación de la dirección de correo electrónico de otras personas o entidades, utilizada generalmente para enviar *spam* o como comienzo de la dinámica de ataque del *phishing.*

- **Ciberespionaje, espionaje informático, o *snooping:*** Funciona mediante la interceptación de comunicaciones tales como correos electrónicos o conversaciones por medio de cualquiera de las redes telemáticas; dirigida tanto a empresas para el descubrimiento de secretos comerciales, como a particulares para la obtención de datos personales.

El espionaje informático se puede realizar de las siguientes maneras:

- Por un *insider* que aprovecha su situación en la empresa o su relación con la persona de confianza para dañarla.
- Por un *hacker* que accede directamente al sistema informático.
- Por medio de todo un *software (como el spyware*) cuya finalidad primera es la obtención de datos de muy diverso tipo y con diferentes objetivos últimos.

- **Ciberblanqueo de capitales y ciberextorsión:** Existen muy diversas técnicas para el blanqueo del dinero virtual, las más comunes hasta la fecha son el uso de mulas para el envío de dinero y el logro de divisas por medio de los juegos online:

- Cuando se habla de las mulas, sobre todo en el ámbito del phishing, se hace referencia a los usuarios de Internet que tienen (o abren) cuentas bancarias, y que son reclutados vía web bajo la apariencia de un contrato de trabajo realizado desde casa, y que consiste en la recepción en sus cuentas bancarias de dinero y su envío, o también por transferencia bancaria, a las cuentas corrientes de los cibercriminales a cambio de una pequeña comisión.
- En cuanto a las webs de juego online, éstas suponen la creación de una economía virtual en las que se intercambia el dinero real por dinero virtual para participar en los juegos.

Por su parte, la extorsión realizada por cibercriminales, generalmente por bandas organizadas, consiste en la solicitud de importantes cantidades económicas a cambio de cesar en la realización de algún tipo de ciberataque o incluso de empezar a ejecutarlo.

Estas conductas parecen proliferar en relación con las páginas web dedicadas a las apuestas y a los juegos de azar online.

- **El ciberacoso:** Es aquel entendido como una macro categoría englobadora de todas las conductas en las que se aprovecha el uso de distintos instrumentos de comunicación como el Messenger, el correo electrónico, el sistema de comunicación oral Skype o las redes sociales como Twitter o Facebook para realizar el atentado contra la libertad de otra persona a través de amenazas, coacciones, injurias, calumnias y otras agresiones al honor.

Aunque el ciberacoso se puede dar de muy distintas formas, las más comunes son:

- **El cyberbullying o ciberacoso escolar o a menores:** Variante del ciberacoso en la que un menor atormenta, amenaza, hostiga, humilla, o molesta de alguna otra manera a otro, haciendo uso de Internet, teléfono móvil, videoconsola o alguna otra tecnología telemática de comunicación, ya sea a través de correo electrónico, mensajes de teléfono móvil (SMS y MMS), mensajería instantánea, blogs, etc.

- **El cyberstalking o ciberacoso continuado propiamente dicho:** Podría entenderse como el uso de Internet u otra tecnología de comunicación para hostigar, perseguir o amenazar a alguien. Se trata de comportamientos en los que un individuo inflige a otros instrucciones o comunicaciones repetidas y no deseadas.
- **El ciberacoso sexual, dentro del cual estaría el online grooming:** Conductas relacionadas con la negación del ejercicio libre de la sexualidad por parte de los adultos y la afectación del proceso de formación de tal libertad sexual en los menores.

Comprendiendo El *cybergrooming* u *online grooming* definido aquí como ciberacoso sexual, todas las conductas preparatorias llevadas a cabo por el abusador sexual hasta lograr el encuentro con la víctima potencial, consistente, generalmente, en un proceso de seducción, bien por medio del envío de mensajes, por e-mail o, más comúnmente, a través de las salas de chat, de algún menor que, por la general inexperiencia de los menores en las relaciones amorosas, y por lo general incapacidad en la fase temprana de la adolescencia (12 a 14 años) para comprender la naturaleza sexual que tienen muchas de las conversaciones, son especialmente vulnerables a este tipo de ataques.

- **La ciberpiratería intelectual:** Es indudable que la popularización del ciberespacio ha conllevado significativas pérdidas de ingresos de la industria de las obras del ingenio, afectada por las nuevas formas de explotación no autorizada de los derechos de autor sobre obras videográficas, cinematográficas, musicales o software, que es lo que se denomina como piratería intelectual.

Paralelamente a lo anterior existe también la llamada piratería digital, o ciberpiratería. Desde la venta directa de obras digitalizadas, pasando por la comunicación pública de las obras vía *streaming* a cambio de una cantidad de dinero, entre otras muchas, Internet ha dado lugar a variadas conductas caracterizadas por la infracción de derechos de propiedad intelectual y que englobarían lo que se viene denominando ciberpiratería.

Sin embargo, sobre el que más podría discutirse su consideración como piratería digital es el intercambio gratuito de archivos.

De hecho, además de la proliferación de sitios de descarga gratuita de archivos y de nuevas formas de explotación, en ocasiones lícitas, pero contrarias a la configuración tradicional de la propiedad intelectual, se une el hecho de que, en los motores de búsqueda como Google, Yahoo! y Bing, muchos de los principales resultados que brindan sus páginas proporcionan enlaces a contenidos no autorizados o sitios que infringen los derechos de autor.

Y todo ello mientras se mantiene el mismo sistema penal que en ningún caso permite sancionar el intercambio gratuito entre usuarios de archivos protegidos.

Esto pese al absurdo que supone que conductas como la distribución física de copias cuya incidencia en la actualidad es casi ridícula para los intereses patrimoniales de los titulares de los derechos, pueden ser sancionadas penalmente. Pero, el intercambio gratuito de archivos llevado a cabo en webs que obtienen gracias a las visitas, abundantes beneficios económicos son difícilmente punibles, además que las mismas van adaptando sus formas de comunicación para huir de la persecución penal de estos comportamientos.

- **Pornografía infantil en Internet:** La 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.

Comprendiéndose, por pornografía infantil, toda forma de representación o promoción de la explotación sexual de los niños, incluidos los materiales escritos y de audio, que se concentren en la conducta sexual o los órganos genitales de los niños.

Distinguiéndose los distintos tipos de comportamientos delictivos, que han conformado la difusión de pornografía infantil, en las siguientes fases:

- **Primera fase:** Se empleaban páginas web alojadas en servidores de Internet, en las que el traficante comerciaba con el material pornográfico infantil que ponía a disposición de los usuarios que previamente accedían a pagar una contraprestación, que se satisfacía por medio de un cargo en la tarjeta de crédito del adquirente cuyo número previamente tenía que proporcionar éste. Aquí se evidencian dos modalidades conductuales:
    - La del usuario de Internet que decide navegar con el objeto de acceder a una página web concreta cuyo contenido sabe con certeza que contiene material pornográfico infantil.
    - La de aquél que crea la página web misma.
- **Segunda fase:** Los chats desarrollados en tiempo real en las que «los pedófilos dialogan entre sí y acuerdan intercambiarse a través del correo electrónico el referido material; la compra directa de este elemento por medio de alguna página web o la simple descarga de archivos en los que el intercambio de fotografías de pornografía infantil es cuestión de segundos.
- **Tercera fase:** La figura del traficante de pornografía infantil es sustituida en gran medida por la de los consumidores que informalmente se asocian sin ánimo de lucro.

Estos socios, actuando coordinadamente, pueden descargarse en su ordenador multitud de fotografías en poco tiempo a través de técnicas de intercambio por medio de correo electrónico o de fórmulas como *send to receive.*

Es por este último tipo de modalidades conductuales que la mera tenencia de material pornográfico infantil para su uso adquiere una mayor importancia, puesto que sin esta posesión de material en los ordenadores de los usuarios no se podría distribuir a los otros usuarios, especialmente en estas redes de P2P, en las que cada nodo funciona al mismo tiempo de servidor y cliente al mismo tiempo.

Por todo ello, además de estas formas de difusión de pornografía infantil, habrá que tener en cuenta otros comportamientos que sin tratarse de «difusión» entran dentro

del fenómeno de la pornografía infantil, como pudieran ser las grabaciones caseras o la mera tenencia de material pornográfico infantil para su uso.

- **Difusión de otros contenidos ilícitos (especial atención al *online hate speech* o difusión por Internet de odio racial):** La posibilidad de introducir información en la Red con contenidos ilícitos diversos y de difundirlos a través de ella, ha convertido a la Red en un medio potente para la comisión de delitos como la apología y otros actos preparatorios del terrorismo.

El denominado *cyberhate speech* o incitación al odio racial en el ciberespacio es uno de los cibercrímenes que más destaca en esta categoría.

Internet ha permitido sustituir prospectos y folletos racistas que eran difundidos localmente, por webs y blogs fáciles de hacer y que resultaban mucho más eficaces para transmitir ideas odiosas a millones de personas en todo el mundo.

A veces tales mensajes se contienen en las mismas webs de asociaciones defensoras de la supremacía blanca u otras ideologías fascistas, y en otros casos, los de las denominadas *cloaked websites*, se tratan de sitios web que aparentan ser de ONG u otras organizaciones preocupadas por problemas sociales de cualquier tipo o que simulan ser lugares de transmisión de información, y que ocultan una ideología racista que va apareciendo poco a poco en forma de mensajes web.

También podríamos integrar dentro de este tipo de cibercriminalidad otras páginas web en las que el mensaje de odio y de incitación a la violencia y de difusión de ideas racistas es menos abstracto y mucho más localizado contra partidos políticos, gobernantes o asociaciones concretas y determinadas.

Tabla 1. *Modalidades del Cibercrimen según Fernando Miró.* En esta clasificación el autor distingue los ciberataques según los distintos intereses sociales afectados y la incidencia de las TICs en el fenómeno criminal.

	CIBERATAQUES PUROS	**CIBERATAQUES REPLICA**	**CIBERATAQUES DE CONTENIDO**
Cibercrímenes Económicos	• Hacking • Malware intrusivo • Malware destructivo • Ataques de insiders • Ataques DoS • Spam • Ciberocupación • Red • Antisocial networks	• Ciberfraudes (phishing, pharming, scam, auction fraud...) • Cyberspyware (uso de sniffers y demás spyware, ciberespionaje de empresa) • Identity theft • Spoofing (DNS spoofing, ARP spoofing, IP spoofing, web spoofing) • Ciberblanqueo de capitales • Ciberextorsión • Ciberocupación	• Distribución de pornografía infantil en internet • Ciberpiratería intelectual
Cibercrímenes Sociales		• Spoofing • Cyberstalking • Cyberbullying • Online harassment (ciberamenazas, coacciones, injurias, etc.) • Sexting (y extorsión con imágenes de sexting) • Online grooming	
Cibercrímenes Políticos	• Ataques DoS (cyberwar) • Ataques DoS (Cyberhacktivism) • Malware intrusivo	• Ciberespionaje terrorista • Ciberguerra	• Online hate speech • Ciberterrorismo (difusión de mensajes radicales con fines terroristas)

Fuente: MIRÓ, Fernando. El cibercrimen. Fenomenología y Criminología de la delincuencia en el ciberespacio. Madrid: Marcial Pons, 2012. p. 51.

No obstante, es posible apreciar otro tipo de agrupación del cibercrimen, más simple, en atención de las propiedades esenciales (confidencialidad, integridad y disponibilidad) de los atentados contra la información; como apreciamos en la doctrina penal, en base a las aseveraciones de[19]:

- **Julio Téllez Valdez:** Quien clasifica a los delitos informáticos en base a dos criterios: *Como instrumento o medio* (referente al empleo de las computadoras como método, medio, o símbolo en la comisión del ilícito) o *como fin u objetivo* (Enmarcando las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física).
- **María de la Luz Lima:** Que distingue la clasificación, de lo que ella llama "delitos electrónicos", en base al empleo de la tecnología electrónica para la comisión del ilícito, a través de las siguientes tres categorías: *Como método* (cuando se utilizan métodos electrónicos para llegar a un resultado ilícito), *como medio* (empleando la computadora como medio o símbolo para la comisión del ilícito) y *como fin* (siendo dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla).

Así mismo, conforme los convenios y tratados internacionales, podremos apreciar otro tipo de catalogalización del cibercrimen, como apreciaremos en[20]:

- **La Convención de Delitos Informáticos del Consejo de Europa de 2001:** La cual clasifica las conductas lesivas a la información en cuatro tipos: *Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos* (sanciona el acceso y la intercepción ilegal, interferencia de datos y sistemas y el mal uso de dispositivos); *Delitos de fraude informático* (falsificación y fraude computacional); *Delitos por su contenido* (producción, diseminación y posesión de pornografía infantil); y *Delitos relacionados con la infracción de la*

19. QUEZADA, Martha. Análisis jurídico de la ley 1042: "Ley especial de ciberdelitos" [En línea]. Nicaragua: Poder Judicial, 2021, p. 15. [Consultado el 10 de junio de 2022]. Disponible en:https://www.poderjudicial.gob.ni/iaej/pdf/Reformas/ANALISIS%20JURIDICO%20LEY%201042.%20LEY%20ESPECIAL%20DE%20CIBERDELITOS.pdf

20. QUEZADA, Martha. Op. Cit. pp. 16-17.

propiedad intelectual y derechos afines (amplia gama de reproducciones ilícitas por medios informáticos de obras protegidas por el derecho de autor).

- **La Propuesta de Decisión-Marco del Consejo Europeo Relativa a los Ataques de los que son Objeto los Sistemas de Información:** Que identifica las siguientes amenazas: Acceso no autorizado a sistemas de información; Perturbación de los sistemas de información; Ejecución de programas perjudiciales que modifican o destruyen datos; Interceptación de las comunicaciones; Declaraciones falsas.
- **Las Naciones Unidas:** Reconoce los siguientes tipos de delitos informáticos: *Fraudes cometidos mediante manipulación de computadoras* (manipulación de datos de entrada, manipulación de programas, manipulación de datos de salida; y fraude efectuado por manipulación informática); *Falsificaciones informáticas* (como objeto y como instrumento); *Daños o modificaciones de programas o datos computarizados* (sabotaje informático, virus, gusanos y bomba lógica o cronológica); y *Falsificaciones informáticas* (acceso no autorizado a sistemas o servicios, piratas informáticos o hackers y reproducción no autorizada de programas informáticos).

Consistiendo la clasificación adoptada por el Estado de Nicaragua para la identificación del cibercrimen en la conjunción de las tipificaciones señaladas por el Convenio de Budapest, Naciones Unidas, y doctrinariamente, por lo establecido por María de la Luz Lima. [21]

1.6. Perfiles de detección del cibercrimen.

La perfilación en el ámbito cibernético nos permite recopilar y analizar información sobre rasgos de comportamiento que han sido moldeados por la evolución tecnológica; para obtener y clasificar información ligada al comportamiento y motivación del ciberdelincuente, y así, poder instaurar procesos judiciales más dinámicos, acordes a las nuevas realidades.

21. QUEZADA, Martha. Op. Cit. p. 18.

Requiriendo para ello, no solo de la especialización penal, sino, de su complementariedad con la criminología, para la elaboración de una adecuada política criminal preventiva que asegure la persecución penal contra el ciberdelito desde el enfoque conductual de la víctima y del victimario, a través de su perfilación, y del análisis geográfico de la incidencia delictiva. [22]

Por lo que, enfocándonos, en las siguientes líneas, en la perfilación cibernética podremos distinguir los siguientes perfiles:

1.6.1. Perfiles del ciberdelincuente en el ciberespacio. [23]

Desde una perspectiva criminológica, la correcta identificación del ciberdelincuente constituye un papel esencial para la adecuada determinación de la política criminal; garantizando la seguridad de los medios de control social formal, mediante la detección temprana de riesgos, para su regularización, prevención y control.

En tal sentido se define, legalmente, al ciberdelincuente, como “aquella persona que comete acciones antijurídicas, en un entorno digital, mediante el uso de instrumentos tecnológicos”, incluyéndose, dentro de dicha calificación, a aquellos cuya actividad ilícita ha evolucionado con la tecnología.

Como el simple ladrón que pasa del mundo real al mundo virtual para seguir a sus objetivos, como bancos y compañías de tarjetas de crédito, cuya principal motivación es el dinero.

No obstante, tan amplia consideración, en cuanto a la perfilación criminal del ciberdelincuente, presenta sus limitantes por la falta de investigación empírica. Señalando en tal sentido, las Naciones Unidas, durante el XII congreso sobre la prevención del delito y justicia penal, la no existencia de un perfil común del ciberdelincuente, debido a las características heterogéneas del ciberdelincuente.

22. MIRÓ, Fernando. Op. Cit. p. 229.

23. PASCUAL, Ivan. Op. Cit. pp. 18-28.

Sin embargo, otros estudios, como el dirigido a América Latina por Digiware durante 2016, han identificado, como denominador común del ciberdelincuente, la predominancia del perfil masculino; constituyéndose el perfil típico del ciberdelincuente tras la figura de un varón, entre los 25 a 35 años, con un mínimo conocimiento informático y tecnológico que le permite considerar la red como un medio ideal para el desarrollo de sus actividades.

Pero, a pesar de ello, esto no es determinante para la perfilación del ciberdelincuente, por lo que para poder proporcionar una perfilación más certera del ciberdelincuente debemos partir de su clasificación, basándose en sus objetivos, habilidades y motivaciones.

Por lo que, deberemos de retroceder hasta el año 1959, donde aparecerá por primera vez el término con que se identifica a la mayoría de los ciberdelincuentes hoy en día, el término hacker; un término bastante complejo gracias a sus subvariantes, que ha de dividirse en dos grupos, a razón de su filosofía (*Black hat hacker; Grey hat hacker;* y *White hat hacker*) y sus tipos (*Cracker; Prehacker; Lammer; Scriptkiddie; Newbie; Wannaber*; Piratas informáticos; y Bucaneros).

Comprendiendo por hacker, a una categoría dentro de los cibercriminales, referente a todo sujeto con altos conocimientos de programación, que se dedican a buscar formas de modificar programas o encontrar pasadizos entre ellos. Desconfiando, por norma, de la autoridad opresora, por considerar que cualquier información útil para el funcionamiento del mundo debería ser ilimitada y gratuita.

Y aunque los hackers tradicionalmente siguen la conocida ética del hacker, que no busca el mal ajeno, sino la autorrealización y estudio de los sistemas informáticos, así como su seguridad; dicha práctica da lugar a situaciones potencialmente peligrosas, y cuya legalidad, en la mayoría de los casos, queda en entredicho, incluso cuando no conllevan un perjuicio ajeno.

Por lo que, con el fin de comprender mejor la figura del hacker, y no caer en el error de encasillar alguno de sus subtipos dentro de un mismo rol, procederemos a

identificar a mayor detalle los perfiles más destacados dentro de esta categoría; comprendiéndose por:

- ***Black hat hacker*:** A los simples hackers, identificados por no seguir ningún tipo de ética de comunidad, y por buscar a menudo un beneficio personal o económico.

El Hacker negro se dedica a buscar la forma de colapsar servidores, entrar en zonas restringidas o tomar el control de sistemas y redes. Se siente orgulloso de demostrar sus habilidades y su grado de autorrealización es mayor cuanto mayor sea el impacto del perjuicio provocado.

- ***White hat hacker*:** Conocido como hacker ético o tradicional. Su mayor fechoría consiste en dejar una tarjeta de visita informando al administrador de las vulnerabilidades o fallos encontrados en su sistema tras una incursión, recurriendo a sus modificaciones, únicamente para el resguardo de su anonimato.

En ocasiones los Hacker Blancos, son sujetos que han formado parte de los Hacker Negros, y que han decidido cambiar sus propósitos maliciosos por el apoyo a los administradores de los sistemas de seguridad y a la lucha contra el Cibercrimen, utilizando los mismos conocimientos para luchar contra estos.

- ***Grey hat hacker*:** Conocido como hacker de sombrero gris. Aunque posee conocimientos comparables a los del Black hat hacker, los utiliza para encontrar vulnerabilidades o fallos en el sistema de seguridad, ofreciéndose a repararlos bajo un beneficio económico, por lo que se dice que su ética es ambigua.
- ***Cracker*:** Son expertos programadores que utilizan sus conocimientos para modificar el comportamiento de sistemas y redes, explotando cualquier vulnerabilidad encontrada, actuando de manera obsesiva e insaciable, guiados por su afán destructivo y ególatra. Por lo que se les ubica dentro de los hackers de sombrero negro.
- ***Phreaker*:** Enfocados principalmente en los sistemas electrónicos. Conocen el funcionamiento de dichas tecnologías, así como sus protocolos de comunicación

y se dedican a alterar el comportamiento de dichos sistemas por placer y en ocasiones con fines económicos.

- ***Lammer*:** Repudiados dentro del colectivo Hacker, son aquellos internautas que se dedican a recopilar información y ejecutar códigos maliciosos buscando el reconocimiento social como Hacker sin tener un conocimiento real del impacto de sus acciones, ni del funcionamiento del código ejecutado.
- ***Scriptkiddie*:** Son simples usuarios de internet con afición a los temas de Hacking, aunque sin demasiados conocimientos al respecto.
- ***Newbie*:** Conocidos como los aprendices de Hacker. Son aquellos novatos que comienzan a leer y experimentar con la información encontrada y que en ocasiones perpetran intrusiones en sistemas débiles, aunque sin mayor trascendencia dados sus escasos conocimientos. Su único objetivo es aprender.
- ***Wannaber:*** Aspirantes a Hacker con poca perseverancia y capacidad técnica, en su gran mayoría inofensivos, que utilizan sus escasos conocimientos para obtener el reconocimiento social fuera de la red.
- **Piratas informáticos:** Dedicados únicamente a la copia y distribución de software, música, juegos y un largo etc. de contenidos de manera ilegal, atentando contra la propiedad intelectual y los derechos de sus propietarios.
- **Bucaneros:** Comerciantes en la red; dedicados a la compra y venta de material ilegal, como identidades, tarjetas de control de acceso, software crackeado, etc.

Y así, una vez identificados los diferentes tipos de hacker, ciberdelincuente habitual, se considera esencial ampliar los perfiles del cibercriminal, en base a las más recientes actividades ciberdelincuenciales; tomando para ello, de la compañía de seguridad informática McAfee, la siguiente catalogalización:

- **Instaladores de *Bots*:** Aquellos cuya intención radica en conseguir el control de un equipo remoto a través de la instalación de un software malicioso (malware).
- ***Carders*:** Se centran exclusivamente en el robo de identidad y en la consecución de fraudes mediante tarjetas de crédito en la red. Considerándose, por tanto, la evolución de los carteristas tradicionales.

- ***Ciberpunks*:** Considerados ciberdelincuentes traviesos; por dedicarse a la alteración de sistemas públicos, con el objeto de mofarse y ridiculizar a aquellos que consideran sus víctimas, ocasionándoles grandes pérdidas, tanto económicas como de imagen. Sin llegar a tener un objetivo lucrativo en sus actos.
- ***Insiders*:** Empleados o exempleados, con motivaciones económicas o personales, que actúan desde dentro de las propias compañías, valiéndose de su experiencia y conocimiento de los sistemas "desde dentro", para acceder, distribuir información confidencial o perjudicar de algún modo a sus empresas.
- ***Phisher, Spammer*:** Especializados en utilizar el correo electrónico como forma o vía de comunicación con sus víctimas. Buscan el beneficio económico a través de engaños y señuelos que llevan a confusión al cibernauta despistado mostrándose como fuentes aparentemente confiables.

Distinguiéndose así, ya de una vez, los diferentes tipos de ciberdelincuentes según su perfil técnico y su filosofía; no obstante, esta lista aún sigue, resultando necesario agregar una última clasificación adicional, en base al papel que desempeña este tipo de individuos.

Entendiéndose, que al igual que en la delincuencia tradicional, esta categoría de delincuentes puede también constituirse en entramados complejos, con estructuras jerárquicas similares a las de una empresa común, contando con especialistas en cada campo, proveedores y por su puesto individuos encargados de la dirección y organización de la misma. Caracterizándose, según la compañía de seguridad Panda Security, en los perfiles siguientes:

- **Programadores:** Desarrollan los *exploits* y el *malware*, que se utilizan para cometer los cibercrímenes.
- **Distribuidores:** Recopilan y venden los datos robados, actuando como intermediarios.
- **Técnicos expertos:** Mantienen la infraestructura de la "compañía criminal", incluyendo servidores, tecnologías de cifrado, bases de datos, etc.

- ***Hackers*:** Buscan aplicaciones *exploits* y vulnerabilidades en sistemas y redes.
- **Defraudadores:** Crean técnicas de ingeniería social y despliegan diferentes ataques de *phishing* o *spam*…
- **Proveedores de *hosting:*** Ofrecen un entorno seguro para alojar contenido ilícito en servidores y páginas.
- **Vendedores:** Controlan las cuentas y los nombres de las víctimas y las proveen a otros criminales mediante un pago.
- **Muleros:** Realizan las transferencias bancarias entre cuentas de banco.
- **Blanqueadores:** Se ocupan de blanquear los beneficios.
- **Líderes de la organización:** Frecuentemente, personas normales sin conocimientos técnicos, que crean el equipo y definen los objetivos.

Por último, cabe destacar, debido a la ambigüedad ética aplicada al mundo de los delitos informáticos, que cualquier persona con acceso a internet puede ser un potencial ciberdelincuente, debido a pequeñas acciones ilícitas, que no suelen perseguidas habitualmente, como es el caso de la propiedad intelectual, que en el mundo online ha perdido, por parte del usuario, su objetividad, al momento de calificar tal conducta como ilícita, provocando se cometa de manera inconsciente por parte de los usuarios, sin catalogarla, ni denunciarlos, como tales. Ejemplo de ello apreciamos, a razón del sinfín de recursos gratuitos e inagotables en internet, la descarga de una canción, un álbum, o una película sin pagar por ello.

1.6.2. Perfiles de la víctima en el ciberespacio.

A este punto, comprendiendo que el campo de acción del cibercrimen habita en la totalidad del ciberespacio, y reconociendo la existencia de un amplio catálogo de tipologías cibercriminales, resulta comprensible la existencia de múltiples víctimas de la ciberdelincuencia.

Comprendiendo que cualquier usuario de internet con acceso, o, mejor dicho, cualquier persona con acceso a un sistema informático, conectado a la red o que, a través de los sistemas existentes en colegios, bibliotecas, universidades,

instituciones públicas, cibercafés, hoteles y demás, puede ser víctima de cibercriminales, de muy distintos tipos, dependiendo de la motivación del sujeto que realiza el ataque, pero, también, del tipo de actividad que el propio usuario realice. [24] Resultando imposible la configuración de un perfil único de la víctima potencial del cibercrimen, por lo que habremos de subsumir tipología, en su generalidad, en los siguientes tres tipos[25]:

- **El ciudadano de a pie:** Cuya permanencia constante en el ciberespacio, correlacionada con su condición de miembro más vulnerable de la sociedad, lo convierte en la víctima principal de la ciberdelincuencia.

Comprendiendo esta condición de vulnerabilidad, en muchas ocasiones, la inconsciencia, por parte del usuario, de los riesgos que supone para sí mismo, la falta de celo y de información en cuanto a las medidas de seguridad aplicadas, ya sea a su sistema informático o a su información confidencial.

Y si bien es cierto, que algunos usuarios, aunque muy pocos, adoptan mecanismos personales para enfrentarse a un ciberdelito, estos no suelen ser útiles, y en muchos casos, ni seguros.

- **Las empresas:** El expansionismo de las actividades comerciales a las vías electrónicas, ha encaminado los principales objetivos, de los ciberdelincuentes, hacia el robo de información confidencial, sea interna o financiera, de la propia compañía; poniendo, consecuentemente, en peligro la seguridad de los usuarios finales.
- **Los gobiernos:** La evolución tecnológica ha significado para los Estados la evolución natural de los métodos empleados en los conflictos entre estados, surgiendo en tal punto figuras como el ciberespionaje y la ciberguerra, que ha resultado objeto de noticia en más de una ocasión.

24. MIRÓ, Fernando. Op. Cit. pp. 261-263.

25. PASCUAL, Ivan. Op. Cit. pp. 29-42.

Comprendiéndose, también dentro de este ámbito, las amenazas de terrorismo, que ahora comparten lugar en el ciberespacio, con casos de Ciberterrorismo, ya sea proveniente de otros países o de bandas organizadas. Suponiendo este nuevo uso de internet por parte de los terroristas, no sólo para perpetrar ataques, sino para captar adeptos y propagar sus ideales, una grave amenaza para la seguridad tanto nacional como internacional.

1.7. Surgimiento de las teorías criminológicas explicativas de la ciberdelincuencia: Consideraciones de Sergio Arroyo. [26]

No es desconocido el tardío interés de la criminología por el estudio del fenómeno criminal de las nuevas tecnologías, tanto a nivel teórico como empírico, por lo que bajo la observancia de las teorías criminológicas tradicionales esta se incursiona en la explicación etiológica del fenómeno ciberdelincuencial, tomando como base diferentes aproximaciones teóricas clásicas, como podremos apreciar a continuación:

- **La teoría del aprendizaje social y la asociación diferencial de SUTHERLAND y AKERS:** Establece la comunicación como fuente de aprendizaje; por lo que advierte que el delito también puede aprenderse mediante un proceso de asociación diferencial. Introduciendo así el término "proceso de contaminación criminógena" como el resultado producente de la accesibilidad de contacto permisivo por las nuevas tecnologías.
- **La teoría del control social, de los vínculos sociales y del autocontrol de GOTTFREDSON & HIRSCHI:** Dispone la capacidad de un individuo para controlar sus impulsos y retener sus deseos como el patógeno primordial de la delincuencia; y advierte que, si el control personal es débil, corresponderá a la carencia de fuerzas socializadoras. Y en relación con el fenómeno cibercriminal

26. ARROYO, Sergio. Estudios criminológicos contemporáneos (IX): La Cibercriminología y el perfil del ciberdelincuente. *Revista de Derecho y Cambio Social* [En línea]. ABR-JUN 2020, Nº. 60, pp. 474-476. [Consultado el 04 de marzo de 2022]. Disponible en: file:///C:/Users/cash%20america/Downloads/Dialnet-LaCibercriminologiaYElPerfilDelCiberdelincuente-7524987.pdf

enfatiza que las nuevas formas de relacionarse han coadyuvado al constante deterioro de los vínculos sociales tradicionales en un mundo, por lo que ha mayor facilidad de interacción online se producirá siempre una contrarespuesta, reflejada en la menor capacidad de comunicación real, en tal sentido, la facilidad de obtención de información o recompensas mediante internet repercute en el individuo, debilitando su capacidad de autocontrol, dando vía libre a los comportamientos delictivos en el ciberespacio.

- **La teoría general de la tensión de AGNEW:** Dicha teoría entrelaza la frustración sufrida individualmente por el rechazo de ciertos estados afectivos con la producción del crimen; instituye la existencia de diferentes fuentes de tensión en base a: la imposibilidad de alcanzar las expectativas sociales deseadas; la privación de estímulos positivos; la sugestión a situaciones negativas aparentemente sin escapatoria. En tal sentido considera que la libertad prometida por el medio cibernético puede servir como vía de escape o superación de las frustraciones a las que es sometido el sujeto en el mundo real.
- **La teoría de las ventanas rotas (Broken Windows) de WILSON & KELLING o de la disuasión de ANWAR & LOUGHRAN:** Altamente influenciada por la carencia del control social ante la comisión de un delito, por lo que desemboca en la idea de desorden o decadencia social, donde la permisiva aceptación de algunas tipologías de cibercrimen, contribuyen a la comisión de nuevos hechos delictivos; por lo que advierte de la inexistencia de métodos eficaces para la detección del delito y la acción de la Justicia, así como de la imprevisibilidad de castigo.
- **La teoría de las actividades rutinarias de COHEN & FELSON y de la oportunidad CLOWARD & OHLIN:** Distingue la cibervictimización en base a tres factores fundamentales (un ofensor motivado, víctimas propicias, y la ausencia de guardianes capaces de actuar contra una vulneración de la norma); por lo que considera la existencia de un proceso de insensibilización, armonizado y favorecido por la impunidad digital, que permite la potenciación de motivación del ofensor, gracias a las brechas de seguridad detectadas. En tal sentido, algunos estudios sugieren que la velocidad de Internet y el acceso a

equipos informáticos tienen un impacto en las oportunidades de los delincuentes para cometer determinados ciberdelitos.

- **La teoría de las técnicas de neutralización de DAVID MATZA y GRESHAM SYKES:** En base a la creencia de la ausencia de generación de daños, algunos hackers justifican sus conductas ilegales en Internet, bajo la premisa de mejorar el propio sistema.

No obstante, es de imperiosa necesidad resaltar que el ciberespacio es una ubicación totalmente nueva que ha creado su propia criminalidad. Por ello, en los últimos años. Algunos autores han tratado de dar respuesta al porqué del cibercrimen a través de novedosas teorías creadas específicamente para el estudio de esta clase de delincuencia.

Fundamentando algunas de estas teorías en la simple renovación de las premisas tradicionalistas y su adaptación al ciberespacio, como podemos ilustrar con:

- ***La Situational Action Theory Revised for the Internet (SAT-RI)* o Teoría de la Acción Situacional revisada paraInternetde WIKSTRÖM,** la cual ha sido estudiada en el contexto digital por PÉREZ SUAREZ: Comprendiendo el internet como único entorno para la propensión individual al delito cibernético, ya que al encontrase compuesto por un contexto moral autónomo, no relacionado con el contexto moral fuera de línea, considera que este tiene su propio conjunto de valores morales y normativos por los cuales se regula a sí mismo.
- **La Ciber Teoría de las Actividades Cotidianas (Ciber TAC) y su Modelo Estructural de Ciber TAC (prevención) de CHOI & TORO-ÁLVAREZ:** Considera el ciberespacio un nuevo ámbito de riesgo criminal, en el que se ven modificados algunos condicionantes relacionados con el delito, por lo que la teoría de las actividades rutinarias añade dos elementos a considerar: a) Estilo de vida digital como factor importante de victimización, compuesto por las distintas actividades en línea; y b) Custodia digital eficiente, en forma de sistemas instalados de seguridad informática, que diferenciaría el nivel de victimización por delitos informáticos.

Otras teorías, sin embargo, parten de una nueva premisa desarrollada específicamente para la explicación del ciberdelito, tal es el caso de:

- **La Teoría de la Transición Espacial de JAISHANKAR:** Que pretende dar una explicación sobre la naturaleza del comportamiento de las personas que ponen de manifiesto su comportamiento conformista y no conformista en el espacio físico y el ciberespacio. Esta teoría integrada sostiene, en suma, que las personas se comportan de manera diferente cuando se desplazan de un espacio a otro.[27]

2. LA CRIMINOLOGÍA.

2.1. Antecedentes históricos.

En el campo criminológico es posible distinguir dos tipos de antecedentes, o bien, fuentes[28], históricos y reales, los cuales observan aspectos que han tenido relación con la criminalidad y que con el tiempo fueron construyendo el estudio propio y directo de la conducta antisocial.

Estas fuentes o antecedentes históricos son aquellas que se estiman como "indicios", es decir, son los que indican la presencia de un fenómeno, pero sin estar estos estrechamente relacionados. En tal sentido, la criminología posee una corta historia como ciencia, pero un largo pasado como conocimiento teórico práctico, este pasado relata la evolución de aquellas acciones llevadas a cabo para explicar el fenómeno criminal y prevenir conductas antisociales por medio de diversos instrumentos.

27. Ibídem. pp. 476-479.

28. PENICHE, Francisco. Introducción al estudio del Derecho. En: HIKAL, Wael. *Introducción al estudio de la Criminología* [En línea]. México: Editorial Porrúa, SA, 2013, p. 24. ISBN: 978-607-09-1475-1 [Consultado el 03 de marzo de 2022]. Disponible en: https://www.scenacriminis.com/wp-content/uploads/2017/09/Introduccion-al-Estudio-de-la-Criminologia.pdf

2.1.1. Fuentes históricas.

Así pues, son considerados como precedentes históricos de la criminología, la religión[29], la cual ha servido como instrumento de prevención de la criminalidad desde siempre. Se destaca que las religiones primitivas hacen referencia a una variedad de comportamientos que constituyen un tipo de conducta, estas sociedades se basaban en dos elementos de gran significación: el *tótem* y el *tabú*.

El *tótem* puede ser una especie de animal o planta, o un fenómeno natural o fisiológico al que un grupo se cree vinculado de determinada forma.[30] Por su parte el *tabú*, es la prohibición de un tema, persona o tipo de conducta, en los tabúes religiosos el tema prohibido se considera sucio.[31] Las prohibiciones relativas al crimen dentro de la sociedad es ejemplo de tabúes de conducta. Entonces, en las sociedades primitivas, la solución al problema criminal era ejercida por medio del *tabú*.

Así mismo, nos es posible apreciar otro antecedente en el distinguido Código de Hammurabi de 1700 a.C. aproximadamente, el cual constituye uno de los documentos rectores que rigió en Oriente por más de mil años y es la recopilación de leyes y órdenes auxiliadas por el rey de Babilonia Hammurabi, por lo cual no es extraño que sea comúnmente citado en diversos textos de criminología, derecho, y

29. Microsoft. Religión. En: HIKAL, Wael. *Introducción al estudio de la Criminología* [En línea]. México: Editorial Porrúa, SA, 2013, p. 25. ISBN: 978-607-09-1475-1 [Consultado el 03 de marzo de 2022]. Disponible en: https://www.scenacriminis.com/wp-content/uploads/2017/09/Introduccion-al-Estudio-de-la-Criminologia.pdf

30. Microsoft. “Tótem” y “Totemismo”. En: HIKAL, Wael. *“Introducción al estudio de la Criminología”* [En línea]. México: Editorial Porrúa, SA, 2013, p. 26. ISBN: 978-607-09-1475-1 [Consultado el 03 de marzo de 2022]. Disponible en: https://www.scenacriminis.com/wp-content/uploads/2017/09/Introduccion-al-Estudio-de-la-Criminologia.pdf

31. Microsoft. Tabú. En: HIKAL, Wael. *Introducción al estudio de la Criminología* [En línea]. México: Editorial Porrúa, SA, 2013, p. 26. ISBN: 978-607-09-1475-1 [Consultado el 03 de marzo de 2022]. Disponible en: https://www.scenacriminis.com/wp-content/uploads/2017/09/Introduccion-al-Estudio-de-la-Criminologia.pdf

muchos más, pues es el primer y uno de los más importantes códigos de la historia, el cual fijó reglas específicas, terminó con la ilegalidad de quienes tenían el poder y protegió a todos los ciudadanos del imperio babilónico.

De igual forma, existen muchos otros acontecimientos históricos, relatos, documentos históricos, antiguos papeles, escritos religiosos y mitológicos (como la misma biblia) que constituyen antecedentes de la criminología, con lo cual se demuestra que la misma siempre ha existido.

2.1.2. Fuentes reales.

Por otra parte, las fuentes reales, son aquellos sucesos, eventos, circunstancias y factores que provocaron el interés para explicar las conductas antisociales y la preocupación por prevenirlas de una forma científica.

En tal sentido, se reconoce como fuentes reales directas a las Ciencias Ocultas, las cuales tuvieron su mayor auge en la edad media y en el renacimiento, y son los antecedentes inmediatos a ciencias modernas como la Psiquiatría, Psicología o la Astrología.

Algunas de estas ciencias son la Demonología, la cual se encarga del estudio de la naturaleza y cualidades de los demonios[32], vinculándose así con la brujería, definida como el conjunto de prácticas mágicas o supersticiosas que ejercen los brujos y las brujas[33], a los cuales se supone dotadas de poderes sobrenaturales que ponen en práctica mediante ritos mágicos, en general para causar un mal; también se le conoce como magia negra o hechicería.

Según Eduardo Lozano Tovar, hasta el siglo pasado se tenía la idea que los delincuentes eran personas malignas, que cometían los peores crímenes sólo por

32. Diccionario de la lengua española, Real Academia Española. Demonología. [En línea] [Consultado el 06 de abril de 2022]. Disponible en: https://dle.rae.es/demonolog%C3%ADa

33. Diccionario de la lengua española, Real Academia Española. Brujería. [En línea] [Consultado el 06 de abril de 2022]. Disponible en: https://dle.rae.es/brujer%C3%ADa?m=form

el placer de hacerlo, en ocasiones estimulados por la fuerza del demonio, esto último según una de las teorías más antiguas que responde a su causalidad del crimen dada por la Teología.[34]

Del mismo modo, desde la antigüedad se ha pensado que los acontecimientos ocurridos en el espacio tenían que ver con el destino de las personas por lo cual se desarrollaron suposiciones de cómo sería el comportamiento de alguien dependiendo del movimiento de los planetas y las estrellas (soles). Así, nace la Astrología, otra ciencia antecesora de la criminología la cual se encarga de observar, analizar y estudiar las posiciones y movimientos de los astros, en especial el sol, la luna, los planetas y las estrellas, relacionándolos con el desarrollo de los acontecimientos que se producen en la Tierra. De esta ciencia sobresalen obras como de Lavater como *La influencia de los planetas sobre el cuerpo humano* e *Informes sobre los descubrimientos del magnetismo animal.*[35]

También es posible hacer mención de la Fisionomía, ciencia encargada del estudio de la apariencia externa de los individuos y la relación entre dicha y su interior, es decir, la relación entre el exterior y el interior de las personas, afirmando que la personalidad, la mente y las emociones de estos se ven reflejadas por medio de los rasgos faciales, expresiones, etc.

De los fisonomistas proviene la expresión: “tiene cara de...”. Ellos señalan que el rostro de las personas puede revelar su carácter delincuencial, el mismo San

34. LOZANO, Eduardo. Manual de Política Criminal y Criminológica. En: HIKAL, Wael. *Introducción al estudio de la Criminología* [En línea]. México: Editorial Porrúa, SA, 2013, p. 60. ISBN: 978-607-09-1475-1 [Consultado el 03 de marzo de 2022]. Disponible en: https://www.scenacriminis.com/wp-content/uploads/2017/09/Introduccion-al-Estudio-de-la-Criminologia.pdf

35. RISOTO, Lucas. Una Aproximación al estudio de lo imaginario en la ilustración: El caso de Franz Antón Mesmer. *Revista de Filosofía* [En línea]. N. 1 2012, pp. 74-75. [Consultado el 06 de abril de 2022]. Disponible en: https://dialnet.unirioja.es/descarga/articulo/6297605.pdf

Jerónimo aconsejaba observar directa mente a los ojos de las personas para conocerlas.[36]

Y es que, en efecto, son muchos los saberes que anticiparon al estudio de la conducta antisocial, tales como la Frenología, la Antropología Criminal y la Sociología Criminal. De lo anterior se afirma que todas las ciencias actuales deben su origen a un cuerpo de conocimientos antecesores que posteriormente se fueron transformando.

2.2. Nacimiento de la criminología como ciencia. [37]

Cada una de las fuentes históricas y reales anteriormente estudiadas constituyen antecedentes de la criminología, con lo cual se demuestra que siempre ha existido, pero no fue hasta cuando el precursor de la Antropología Criminal, el médico Franz Josef Gall expuso su teoría de que el comportamiento tiene bases en las funciones del cerebro, que la criminología fue considerada como un conocimiento sistemático.

Posteriormente, el médico César Lombroso, retomó dichas teorías y estudió a los criminales en sus características biológicas interiores (desórdenes congénitos) y exteriores (características físicas); además de las psicológicas y las sociales. Y es así como el 15 de abril de 1876, algunos consideran la fecha oficial del nacimiento de la Criminología como ciencia, ya que ese día se publica el *Tratado Antropológico Experimental del Hombre Delincuente*, en el cual Lombroso expone su teoría.

Lombroso hizo la clasificación más importante de los delincuentes que ha servido como base para posteriores clasificadores. Atendiendo a sus observaciones, formula una serie de categorizaciones de sus analizados, separándolos en: Anatómicos, Fisiológicos, Psíquicos y Sociales.

---

36. ALVAREZ, Germán; MONTENEGRO, María y MARTÍNEZ, José. “Notas para la historia de la criminología”. [En línea]. México: Facultad de Psicología, UNAM, 2012, p. 10. [Consultado el 15 de abril de 2022]. Disponible en: http://www.psicologia.unam.mx/documentos/pdf/publicaciones/Notas_para_la_Historia_de_la_Criminologia_Alvarez_Diaz_Montenegro_Nunez_Martinez_Manuel_TAD_7_8_y_9_sem.pdf

37. Ibídem. pp. 14-20

Por otro lado, Garófalo fue quien se ocupó de popularizar el término “Criminología”, encargándose de la sistematización jurídica de la escuela positivista, con el apoyo de Pablo Toppinard al escribir el libro *La Criminología.*

Antes de formar parte de la Escuela Positiva, Garófalo, había ya publicado algunos escritos, que serían de mucha importancia para la nueva escuela, pues daban las bases y la orientación jurídica necesaria, además de conceptos como: peligrosidad y prevención especial y general.

Sin duda la gran preocupación de Garófalo fue la aplicación de la teoría Criminológica a la práctica, tanto en el aspecto legislativo como en el judicial, así, formula el primer esquema de las penas de acuerdo ya no al delito, sino a la clasificación de los delincuentes. Es así como publicó diversas obras como *Estudios recientes sobre la Penalidad* y, *Criterio Positivo de la Penalidad,* formando parte también de diversos congresos internacionales y sentando las bases para la nueva escuela y la criminología actual.

Por último, Ferri, fue el encargado de aportar la sociología criminal, presentando su tesis en la que trata de demostrar que el libre albedrío es una ficción, y que debe substituirse la responsabilidad moral por una responsabilidad social. Además, trazó las líneas fundamentales de la escuela, reuniendo, en un sistema orgánico y completo, las ideas enunciadas por Lombroso y Garófalo.

Publicó la obra *Los nuevos horizontes del derecho y del procedimiento penal*, donde se señalan el método a aplicar y el área en que deben ser investigadas las causas del fenómeno criminal, las características que ha de reunir la pena para servir a los fines de defensa social, y se sugieren incluso los medios indirectos para prevenir la delincuencia, lo cual puede ser considerado como la partida de nacimiento de la nueva escuela.

Fue así como con los factores de carácter biológico y de naturaleza, sobre todo hereditarios, de Lombroso; con la acentuación del papel de los factores psicológicos de Garófalo; y con la influencia de los factores sociológicos de Ferri, y a través de

estudios, observaciones y experimentos, se proyectó dar explicación a las conductas antisociales de manera científica, conductas que han ido evolucionando en nuevas formas y técnicas de delincuencia.

2.3. Concepto de ciencia criminológica.

No existe una determinación conceptual de la Criminología unitariamente vinculante o predominante. Sin embargo, pese a las divergentes acentuaciones, las opiniones sobre qué es lo que se entiende en la actualidad por Criminología no difieren mucho.

Dicho esto, en las sucesivas líneas, se proporcionarán algunos conceptos aportados por diversos autores clásicos y contemporáneos que permiten comprender de manera más certera su razón de ser.

Así pues, Alessandro Baratta indica que la Criminología tiene como función específica, cognoscitiva y práctica, individualizar las causas de la diversidad de delitos y los factores que determinan el comportamiento criminal, para combatirlos con una serie de medidas que tienden, sobre todo, a modificar al delincuente. [38]

Por su parte, Jorge López Vergara señala que la Criminología es la ciencia que se encarga de estudiar el delito como conducta humana y social, de investigar las causas de la delincuencia, la prevención del delito y el tratamiento del delincuente. [39]

Para Robert Winslow y Sheldon Zhang, la Criminología puede ser definida sencillamente como el estudio de las causas del crimen y la conducta criminal,

38. BARATTA, Alessandro. Criminología Crítica y crítica al Derecho Penal. En: HIKAL, Wael. *Introducción al estudio de la Criminología* [En línea]. México: Editorial Porrúa, SA, 2013, p. 138. ISBN: 978-607-09-1475-1 [Consultado el 03 de marzo de 2022]. Disponible en: https://www.scenacriminis.com/wp-content/uploads/2017/09/Introduccion-al-Estudio-de-la-Criminologia.pdf

39. LÓPEZ, Jorge. Criminología. En: HIKAL, Wael. *Introducción al estudio de la Criminología* [En línea]. México: Editorial Porrúa, SA, 2013, p. 138. ISBN: 978-607-09-1475-1 [Consultado el 03 de marzo de 2022]. Disponible en: https://www.scenacriminis.com/wp-content/uploads/2017/09/Introduccion-al-Estudio-de-la-Criminologia.pdf

incluyendo el estudio de la justicia criminal, en el supuesto de que ésta determina el crimen, y en otros casos, puede producirlo. [40]

2.4. Características de la criminología.

- **Pluridisciplinar:** Cuenta con multiplicidad de competencias y conocimientos.
- **Interdisciplinaria:** Se relaciona necesariamente con otras ciencias o disciplinas.
- **Método utilizado:** Hace uso del método científico para llevar a cabo su estudio.
- **Base de su investigación:** Se fundamenta en mayor medida en la observación de los fenómenos criminales y todos lo que este implica, y no tanto en argumentos u opiniones.
- **Método en el que se apoya:** Se auxilia del método inductivo, el cual tiene su fundamento en el análisis, así como en la observación de la realidad.
- **Objeto de estudio:** Se centra en todas las variantes de la delincuencia.
- **Enfoque:** Está orientada a la prevención o reducción de los fenómenos delictivos.

2.5. Objeto de estudio de la criminología.

- **El delito:** Acción u omisión humana imprudente o dolosa que tiene relevancia penal, es decir, que es contraria a la ley.[41]

40. WINSLOW, Robert & ZHANG, Sheldon. Criminology. En: HIKAL, Wael. *Introducción al estudio de la Criminología* [En línea]. México: Editorial Porrúa, SA, 2013, p. 138. ISBN: 978-607-09-1475-1 [Consultado el 03 de marzo de 2022]. Disponible en: https://www.scenacriminis.com/wp-content/uploads/2017/09/Introduccion-al-Estudio-de-la-Criminologia.pdf

41. Diccionario económico. Delito. [En línea] [Consultado el 07 de abril de 2022]. Disponible en: https://economipedia.com/definiciones/delito.html

- **El delincuente:** Autor de una infracción, es decir, de cualquier acto previsto y castigado por la ley penal y que puede ser objeto de una investigación en este campo.[42]
- **La víctima:** Personas que, individual o colectivamente, hayan sufrido daños, inclusive lesiones físicas o mentales, sufrimiento emocional, pérdida financiera, o menoscabo sustancial de los derechos fundamentales, como consecuencia de acciones u omisiones que violen la legislación penal vigente o normas internacionales relativas a los derechos humanos.[43]
- **El control social:** Concepto utilizado en la sociología, la criminología y la ciencia penal para designar el control de la sociedad frente a conductas desviadas e indeseadas.[44] (concepto que será ampliado en párrafos posteriores)

Pese a lo descrito, los campos de estudio de la criminología no han sido siempre los mismos, sino que son el resultado de una constante evolución, tal como se verá y explicará a continuación.

2.6. Ampliación del objeto de estudio de la criminología.

Tradicionalmente la criminología se dedicó al estudio del sujeto infractor, es decir, del delincuente y consecuentemente del acto delictivo, ignorando interesadamente otros sujetos y elementos de la criminalidad, sin embargo, la moderna criminología en un afán por hacer frente al tratamiento del problema criminal ha ampliado su propio objeto de estudio tomando en consideración al sistema de control social como su nuevo centro de interés en la investigación criminológica con el fin de proporcionar pautas que permitan prevenir y sancionar el delito acorde a la realidad

42. Diccionario Jurídico de Derecho, Enciclopedia Jurídica. Delincuente. [En línea] [Consultado el 07 de abril de 2022]. Disponible en: http://www.enciclopedia-juridica.com/d/delincuente/delincuente.htm

43. Diccionario Jurídico, La Voz del Derecho. Víctima. [En línea] [Consultado el 07 de abril de 2022]. Disponible en: https://lavozdelderecho.com/index.php/actualidad-2/corrup-5/item/2822-diccionario-juridico-concepto-de-victima-en-el-derecho-internacional

44. Diccionario Prehispánico del Español Jurídico. Control Social. [En línea] [Consultado el 07 de abril de 2022]. Disponible en: https://dpej.rae.es/lema/control-social

criminal sin detrimento de los derecho humanos y, asimismo, brindar mejor protección a las víctimas como sujetos pasivos del fenómeno delincuencial.

Dado que en la presente investigación el control social es el tema de preocupación y considerando que en un inicio fue un aspecto y dimensión no ponderado, se hará referencia a él y a su surgimiento de acuerdo a la criminología moderna en las páginas que subsiguen.

3. EL CONTROL SOCIAL.

3.1. Origen de la categoría de control social.

La paternidad científica de la expresión *Control Social* pertenece al sociólogo norteamericano Edward Ross, en la segunda mitad del siglo XIX en los EE. UU.; el cual surge con el objetivo de integrar socialmente las grandes masas de inmigrantes que acudieron a la convocatoria generada por el proceso de industrialización en ese país.

La demanda organizativa de esta población de migradores, caracterizada por su variedad cultural y religiosa, creó la necesidad de localizar las vías sociológicas de integración que superaran estas diferencias y que, a partir del desarrollo de normas comportamentales, garantizaran una convivencia social organizada.[45]

El sentido otorgado por Ross a este nuevo concepto excluía de cierto modo los controles estatales, tanto legales como políticos. Desde esta perspectiva, la esencia controladora sería asumida por la sociedad a través de la interacción social persuasiva, de la cual se derivaba el modelamiento de la conciencia individual a las

45. BERGALLI, R. Relaciones entre Control Social y Globalización: Fordismo y disciplina, postfordismo y control punitivo. En: AGUIRRE, Eduardo. *Control Social* [En línea]. Seminario sobre aportaciones teóricas y técnicas recientes. Universidad Nacional de la Pampa, 2008, pp.7-8 [Consultado el 03 de marzo de 2022]. Disponible en: http://www.biblioteca.unlpam.edu.ar/rdata/tesis/e_puecon623.pdf

necesidades de su entorno, produciéndose entonces un proceso de asimilación e internalización individual de las normas culturales.[46]

La posterior evolución de esta categoría se encuentra en la influencia ejercida por la “Escuela de Chicago”, más concretamente en autores como Park, Mead, Dewey y Burgess. Es en esta escuela donde se distancia la idea del Control Social de aquellas estrategias disciplinarias que pudieran surgir desde el Estado, las cuales son tomadas como de Control Público.

Posteriormente, la posición anterior sustentadora de la exclusión estatal del Control Social resultó superada por los condicionamientos objetivos impuestos en ocasión de la necesidad surgida de las consecuencias de la Gran Depresión Económica de EE. UU. (1929- 1930); motivo por el cual el Estado Norteamericano comienza a asumir el papel de centralizador estratégico del control, principalmente a través del Derecho como instrumento regulador por excelencia.

3.2. Concepto de control social.

El control Social en términos pragmáticos, busca mantener a las conductas negativas dentro de un límite de tolerancia social, a fin de que no afecte la funcionalidad de las instituciones básicas comunitarias. En este sentido, se ofrecen algunos conceptos que reflejan con mayor amplitud la trascendencia de este término y su propósito.

Según Luis Rodríguez Manzanera, el control social puede entenderse como el conjunto de instrumentos (generalmente normativos), instituciones, agentes y

46. BERGALLI, R. La violencia del Sistema Penal. En: AGUIRRE, Eduardo. *Control Social.* [En línea]. Seminario sobre aportaciones teóricas y técnicas recientes. Universidad Nacional de la Pampa, 2008, pp.10-13 [Consultado el 03 de marzo de 2022]. Disponible en: http://www.biblioteca.unlpam.edu.ar/rdata/tesis/e_puecon623.pdf

acciones encaminadas al cumplimiento de los fines y valores propuestos por el sistema imperante, logrando en esta forma mantener el orden social.[47]

Aniyar De Castro afirma que el Control Social es el conjunto de sistemas normativos (...), cuyos portadores, a través de procesos selectivos (...), y mediante estrategias de socialización (...), establece una red de contenciones que garantiza la fidelidad (...) de las masas, a los valores de un sistema de dominación.[48]

Por otra parte, Stanley Cohen considera que el control social se refiere a las formas organizadas en que la sociedad responde a comportamientos y a personas que contempla como desviados, problemáticos, preocupantes, amenazantes, molestos o indeseables de una u otra forma.

Esta respuesta aparece de diversas formas: castigo, disuasión, tratamiento, prevención, segregación, justicia, resocialización, reforma o defensa social y está acompañada de muchas ideas y emociones: odio venganza, desquite, disgusto, compasión, salvación, benevolencia o admiración.

El comportamiento en cuestión es clasificado bajo diversas denominaciones: crimen, delincuencia, desviación inmoralidad, perversidad, maldad, deficiencia o enfermedad. La gente a la cual se dirige esta respuesta es vista como monstruosa, boba, villana, enferma, rebelde o víctima. Y aquellos que responden (haciendo algo o estudiando la materia, tareas que habitualmente se confunden), son conocidos como jueces, policías, asistentes sociales, psiquiatras, psicólogos, criminólogos o sociólogos de la desviación…[49]

47. LÓPEZ, Luis. Sistema y Control Social: Enfoque general. *Revista SAPERE* [En línea]. ENE-MAY 2015, No. 8, p. 5 [Consultado el 01 de marzo de 2022]. Disponible en: https://derecho.usmp.edu.pe/instituto/revista/articulos/2012/Control_Social.pdf

48. ANIYAR DE CASTRO, L. Notas para la discusión de un control social alternativo. Citado por: Viera, Margarita. Lecturas Complementarias sobre Criminología. En: AGUIRRE, Eduardo. *Control Social* [En línea]. Seminario sobre aportaciones teóricas y técnicas recientes. Universidad Nacional de la Pampa, 2008, p. 21 [Consultado el 03 de marzo de 2022]. Disponible en: http://www.biblioteca.unlpam.edu.ar/rdata/tesis/e_puecon623.pdf

49. AGUIRRE, Eduardo. Ensayo de Criminología Crítica Argentina. En: AGUIRRE, Eduardo. *Control Social* [En línea]. Seminario sobre aportaciones teóricas y técnicas recientes. Universidad

Cabe destacar que anteriormente el concepto de control social se utilizaba para designar indistintamente tres problemas:

- El problema clásico de la sociología anterior al siglo XX, esto es, el control social como forma de conseguir y conservar el orden social;
- Las cuestiones de psicología social propias de la sociología norteamericana, fundamentalmente de la corriente funcionalista que estudiaba los procesos de socialización e internacionalización de las normas como formas de control social y;
- El de la escuela que lo percibe como reacción a la desviación

Adicionalmente, en el pasado, el uso del concepto de control social nunca fue neutral, sino que designaba toda actividad estatal, pero en clave de represión, opresión, control, siempre dirigida por el Estado.

Posteriormente se fue atenuando el poder atribuido al Estado en cuanto a la configuración de la reacción social, de tal manera que, si la reacción es precisamente social, la capacidad del Estado para atribuir cuándo y cómo se debe proceder, debe estar en concordancia con aquello que la población asiente, destacando así el papel preponderante de algunos grupos sociales.

3.3. Características del control social.

- **Normativo:** A través del control social se estatuyen normas de diversas tipologías, algunas de obligatorio cumplimiento y otras que no cuentan con poder coercitivo, pero que buscan el mismo fin, esto es, regular el comportamiento de los individuos y mantener el orden social.
- **Sancionador:** Cuando se produce una violación a las normas del control social, se imponen sanciones, las cuales variarán según el tipo de norma que se haya violado.

Nacional de la Pampa, 2008, pp.18-20 [Consultado el 03 de marzo de 2022]. Disponible en: http://www.biblioteca.unlpam.edu.ar/rdata/tesis/e_puecon623.pdf

- **Uniformador:** El control social busca que los individuos que integran la sociedad actúen conforme a las normas establecidas y dejen a un lado su conducta antisocial.

3.4. Formas organizativas de control social.

Como bien se ha sustentado, clásicamente se atribuía el uso del concepto de control social al Estado, de tal manera que era este el único que podía ejercerlo, actualmente estos paradigmas han quedado superados, pues se considera que la multivariada intervención del Control Social se encuentra condicionada por su capacidad de interpenetración en todo el tejido social, generándose multiplicidad de campos de incidencia; lo que propicia una compleja organización operacional y consecuentemente doctrinal del Control Social.

Es así como han surgido distintas formas organizativitas de control social o clasificación de las mismas, siendo la mayormente aceptada aquella que las divide en dos variantes o formas: el control social informal y el control social formal.

3.4.1. Control social formal.

El control social formal descansa en el aparato jurídico, es decir una organización formal encargada de responder a los quebrantamientos de las leyes establecidas a través de las cortes de justicia, el uso de la fuerza pública y la emisión de sentencias para castigar los crímenes cometidos por las personas.

Este tipo de control se caracteriza por tener al Estado como autoridad política principal pues es el poseedor de la exclusividad represiva en su totalidad, lo que se conoce como monopolio legítimo de la fuerza[50], el cual a través del marco jurídico

50. QUIRÓS, R. Manual de Derecho Penal I. En: GONZÁLEZ, Marta. *El control social desde la criminología* [En línea]. Cuba: Editorial Feijóo, 2010, p. 30. ISBN: 978-959-250-582-7 [Consultado el 03 de marzo de 2022]. Disponible en:https://dspace.uclv.edu.cu/bitstream/handle/123456789/12302/Control_Social-1.pdf?sequence=1&isAllowed=y

promulgará qué acciones se deben hacer y qué acciones no se deben hacer a fin de garantizar el orden social.

La presión de este control se ejerce a través de procedimientos y órganos públicos (El derecho y los organismos oficiales que dictan y aplican las normas jurídicas) siendo imperativo y represivo hacia quienes no acatan las reglas o las quebrantan.

3.4.2. Control social informal.

El control social informal consiste en todos los mecanismos y prácticas que se realizan de manera ordinaria en la vida diaria y que generan una presión en los grupos sociales para que sus acciones tiendan a no romper el orden.

Nos referimos a un control en el cual no existe coercibilidad, hablaríamos entonces de un control social mediato equivalente a la manipulación ciudadana a partir de la economía, de lo religioso, de lo educativo, lo recreacional, es decir, con base en las instituciones y medios de difusión encargados de moldear la opinión pública.

Estas instancias de control informal tratan de educar e integrar al individuo en la normativa de orden y consenso[51], interiorizando las pautas y modelos de conducta transmitidos y aprendidos.

3.5. Agencias de control social.

Las agencias de control social son aquellas entidades colectivas, organismos o grupos humanos que juegan funciones de control en la sociedad.

51. GARCIA-PABLOS, Alessandro. Introducción a la Criminología. En: CAVERO, Pedro. La criminología y la ineficiencia del control social frente a la realidad peruana. *Revista electrónica del Centro de estudios de Criminología de la USMP* [En línea]. N. º 3, p. 4. [Consultado el 17 de marzo de 2022]. Disponible en: https://www.usmp.edu.pe/derecho/centro_inv_criminologica/revista/articulos_revista/2013/Criminologia_Ineficiencia_Control_Social.pdf

La característica común que los aúna bajo el rubro de agencias del control es su función particular o combinada de intervención en el logro del orden y la estabilidad social, estas agencias pueden ser formales o informales.

Es imperativo aclarar que cuando las instancias informales del control social fracasan, es cuando entran en funcionamiento las instancias formales, que actúan de modo coercitivo e imponen sanciones cualitativamente distintas de las sanciones sociales: sanciones estigmatizantes que atribuyen al infractor un singular status (desviado, peligroso, delincuente, etc.)[52]

3.5.1. Agencias formales de control social.

Las agencias formales de control social constituyen un conjunto de instituciones dedicadas a promover la conducta socialmente aceptable a través de la amenaza o uso efectivo de la coacción legal.

De esta manera, el control formal, es aquel que se ejerce por las instituciones que integran el sistema penal, como, por ejemplo: la Policía, Poder Judicial, Ministerio Publico y Administración Carcelería, entre otras.

3.5.2. Agencias informales de control social.

El control social informal funciona a través de un largo y sutil proceso que comienza en los núcleos primarios, familia, escuela, colegio, universidad, profesión, centro de trabajo, los medios de comunicación etc. y culmina con la obtención de su actitud conformista interiorizándole las pautas de conducta transmitidas y aprendidas, lo que conocemos como proceso de sociabilidad.

3.6. Control Social Penal.

El control social, como bien se ha afirmado, tiene como objetivo mantener a grupos sociales dentro de un orden formalmente aceptado de modo tal que se respeten un

52. Ibídem

número de normativas básicas que contribuyan a generar estilos de vida organizados y no conflictivos.

En este sentido, las regulaciones más visibles respecto a la idea de control social son aquellas que se expresan a través de leyes, estatutos y regulaciones formales que todos los miembros de una sociedad deben cumplir de igual modo, se hablaría entonces del control social penal.

El control social penal es un subsistema en el sistema total de control social. Su especificidad deriva del objeto a que se refiere, no a toda la conducta desviada sino sólo al delito, así como a sus fines, prevención y represión y a los medios que utiliza para ello, las penas y medidas de seguridad, con una rigurosa formalización en su forma de operar acorde al principio de legalidad, por tal razón, el control social penal se compone como una modalidad del control social formal.

El control social penal se sirve de un particular y propio sistema normativo, que traza pautas de conducta al ciudadano imponiéndole mandatos y prohibiciones, en efecto, el control penal en las sociedades que poseen una organización jurídica constitucional y un Estado de Derecho, nace precisamente a través de la institucionalización normativa, es decir, del derecho penal, el cual está constituido de un conjunto de normas a partir de las cuales la conducta de las personas puede ser valorada como no deseable por lo grupos hegemónicos de poder que consideran que debe ser punible.

De esta manera el control social penal acciona mediante una fuerza imperiosa para hacerse cumplir; entronizándose como un mecanismo exterior coercitivo que presupone un sometimiento de la voluntad individual a la fuerza del Derecho. Todo el accionar controlador que implique el uso del Derecho Penal se canaliza e instituye mediante el funcionamiento del Sistema Punitivo o Sistema de Justicia Penal.

Este tipo de control no debe estar dirigido sólo a la efectividad, sino que debe tener en cuenta también los principios valorativos que informan la intervención del derecho penal en el control de la desviación, el cual tiene como misión la reafirmación y el aseguramiento de las normas fundamentales de la sociedad y la

de cultura jurídica, misión que sólo se puede realizar reforzando los valores ético-sociales de la acción y afianzando el reconocimiento normativo.

3.7. El control social desde la moderna criminología.

La criminología positivista –como se señaló en el apartado sobre la ampliación del objeto del estudio de la criminología— volcada en la persona del delincuente, no prestó excesiva importancia a los problemas del control social.[53]

Los teóricos de la criminología positivista no cuestionan las definiciones legales o la norma, ni aquello a lo que estas responden, mucho menos critican el funcionamiento del sistema legal aplicado a la realidad.

Sino que por el contrario asumen que en ellas descansan efectivamente los intereses generales de la sociedad y que las leyes solo plantean un problema de interpretación reservado al Juez, asimismo, que el sistema legal se basa únicamente en subsumir el caso concreto al presupuesto de la norma, en otras palabras, en encasillar dentro de una clasificación legal una determinada acción delictiva, en cuyo proceso no se experimentan desviaciones significativas, o dicho de otra manera, mayor conflicto, dado el dogma de la igualdad ante la ley.

En tal sentido, el denunciante, las agencias de control y el proceso como tal, son simples correas trasmisoras que aplican fiel y objetivamente la voluntad de la ley.

Siendo la población penitenciaria o reclusa una muestra de la población criminal real a los cuales el sistema se encarga simplemente de detectar y castigar por las acciones cometidas.

53. GARCÍA-PABLOS, A. Manual de Criminología. Introducción y teorías de la criminalidad. En: GARCÍA-PABLOS, A. *La Aportación de la Criminología* [En línea]. Cuaderno del Instituto Vasco de criminología, San Sebastián N. 3, 1989, p. 84. [Consultado el 06 de abril de 2022]. Disponible en: https://www.ehu.eus/documents/1736829/2163271/09+-+La+aportacion+de+la+criminologia.pdf

En efecto, en la criminología moderna, lo decisivo es como operan determinados mecanismos sociales encargados de atribuir el status social, es decir que, la calificación jurídico penal de la conducta como tal pasa a un segundo plano.

De igual manera, más importante que la interpretación de las leyes es analizar el proceso de concreción de las mismas a la realidad social, pues muchas veces el mandato abstracto de la norma se desvía sustancialmente al pasar por el colador de ciertos filtros selectivos y discriminatorios que actúan mayormente guiados por el criterio del status social del infractor.

Precisamente por esto el control social no solo se encarga de detectar la criminalidad y al infractor, sino que, además, termina creando o configurando la criminalidad misma, pues el sistema se orienta prioritariamente a aquellas clases sociales con mayores niveles de criminalidad, o, mejor dicho, el control social se dirige en contra de estas bajo un supuesto de prejuicio.

Contrario a lo señalado por los criminólogos positivistas y según la moderna criminología, las leyes no son la encarnación de los intereses generales de la sociedad y tampoco es cierto que el dogma de la igualdad de la norma hace efectivo el proceso de aplicación de esta, en igual circunstancia, las agencias de control, en este caso formales, no son –hablando del deber ser— simples correas de transmisión, sino que son delegados al servicio de una sociedad desigual para suprimir las injusticias que la caracterizan y por esta misma razón la población penitenciaria no debe considerarse como población criminal real.

4. POLÍTICA CRIMINAL.

4.1. Aspectos generales de la política criminal.

La política criminal es una disciplina que comprende diversas aristas del saber, afín de lo criminológico y del derecho penal, por lo que resulta ineludible comprender sus fundamentos, debido a su complejidad, para garantizar un enfoque más completo y claro de su finalidad e importancia.

En tal sentido, se ha procurado facilitar un acercamiento de lo que, en su generalidad, comprende la política criminal, mediante los siguientes apartados:

4.1.1. Desarrollo histórico de la política criminal.

Históricamente la concepción de Política Criminal tuvo su origen según la dogmática penal a finales del siglo XVII y comienzos del siglo XIX, aunque en Alemania no se logró precisar la fuente doctrinaria autorizada para definirle; siendo objeto de múltiples discusiones en cuanto a su finalidad y condición científica, sin escapar a esto su noción misma, adjudicándosele tanto a Quistorp, como a Kleinshrod, Henken y Feuerbach.

Captando mayor notoriedad, para muchos, a partir de 1800, donde se hace presente en el Derecho Penal con Franz Von Liszt, mediante su distinguida frase “El Derecho es la Infranqueable Barrera de la Política Criminal”, interpretándole como una disciplina autónoma, lógica, sistematizada y de carácter no efímero, dispuesta a permanecer en el desarrollo evolutivo social desde siempre, y cuyo entendimiento sería la clave para poder comprender posibles problemas que necesariamente serán provistos en la sociedad.[54]

Confundiéndose en ese entonces su finalidad con la Criminología, producto de la resistencia alemana.

Y es así como en 1925 se afirma que la Política Criminal no es una disciplina independiente, determinándole una interpretación estrictamente penal, dimitiendo de su sentido social, volviéndose foco críticas, al establecer un concepto de la Política Criminal como suplantación de la Política de Gobierno. Por lo que Desde

54. MOREIRA, Darwin. *Evolución de la Política Criminal* [En línea]. Tesis de titulación en Jurisprudencia y Título de Abogado. Universidad Nacional de Loja. Ecuador, 2016, pp.4-7 [Consultado el 03 de marzo de 2022]. Disponible en: https://dspace.unl.edu.ec/jspui/bitstream/123456789/16904/1/Darwin%20Daniel%20Moreira%20Celi.pdf

entonces en Alemania la dependencia de esta política se acentuaba entre los estudiosos del Derecho Penal.

Prosiguiendo así la transfiguración de dicho término, entre oscilaciones conceptuales, de las ciencias penales y criminológicas, adecuándose cada vez más a la época, así hasta perfeccionarse en un enfoque más casualista.

Siendo, en 1940 cuando el panorama mundial se transforma, tras el el inicio y la creación de la política criminal de las Naciones Unidas, la cual trajo consigo nuevos cambios en la sociedad, influyendo en la imposición de otras fuerzas y la adquisición de un mayor auge de la Declaración Universal de los Derechos Humanos, ocupando un lugar primordial en la Política Criminal.[55]

No obstante, esto condescendió en la ilustración de la Política Criminal, meramente teórica, apreciándose en Francia con Marc Ancel en 1954 con la elaboración de la intitulada “Tesis de la Defensa Social y una Política Criminal más Humanista”; produciéndose en 1974, bajo la presidencia de Ancel, una mesa redonda en donde la noción y extensión de la Política Criminal fueron examinadas, distinguiéndose así, en 1975, la Política Criminal como parte integrante de la Política General.

Y En 1984 se da una marcada referencia sobre la Fundación Internacional Penal y Penitenciaria, en que se editó el coloquio de Siracusa de 1982; dichas tendencias señalaron la descriminalización sobre todo lo que atañe a delitos sexuales y los menores contra la sociedad marcando escepticismo en el Consejo de Europa con respecto a los programas de rehabilitación.

Cabe destacar que en Iberoamérica también debe de citarse la Política Criminal Latinoamericana de Raúl Zaffaroni, quien plantea que la Política Criminal necesita de la participación directa del pueblo, y que es precisa para discusión pública,

55. FONSECA, Xóchitl y FONSECA, Rosalba. *Política Criminal y Sistema Penitenciario Nicaragüense* [En línea]. Tesis de titulación de licenciatura en Derecho. UNAN-León, 2007, pp.1-3 [Consultado el 03 de marzo de 2022]. Disponible en: http://riul.unanleon.edu.ni:8080/jspui/retrieve/3034

debate y contradicción haciendo así efectiva la preservación de los Derechos Humanos. [56]

4.1.2. Definición de política criminal.

Como a bien resalta Emma Morales en su estudio intitulado “Algunas reflexiones sobre política criminal y sus principales tendencias” la política criminal comprende, y cito: “Un conjunto de principios fundados en la investigación científica del delito y de la eficacia de la pena, por medio de los cuales se lucha contra el crimen, valiéndose no sólo de los medios penales, sino también de los de carácter privativo.[57] Así, se ha pretendido lograr resultados de efectividad en la prevención de la criminalidad, dentro de los cánones del respeto a los derechos fundamentales.[58]

No obstante, nos advierte sobre la pertinente diferenciación de la política criminal en contraste con la política penal, por referirse esta última a la respuesta circunscrita en el ámbito del ejercicio de la función punitiva del Estado; distinguiéndose de la política criminal gracias al carácter social que le reviste, por tanto nos proporciona las medidas y criterios de carácter jurídico, social, educativo, económico, establecidas por los poderes públicos para prevenir y reaccionar frente al fenómeno criminal, con el fin de mantener bajo límites tolerables los índices de criminalidad en una determinada sociedad.[59]

---

56. Ibídem. pp.3-5.

57. JIMÉNEZ, Luis. Principios de derecho penal: La ley y el delito. En: MORALES, Emma. Algunas reflexiones sobre política criminal y sus principales tendencias. *Revista Nuevo Derecho* [En línea]. Enero-junio de 2010, No. 6, p. 2. [Consultado: 04 de marzo de 2021]. Disponible en: file:///C:/Users/cash%20america/Downloads/Dialnet-AlgunasReflexionesSobrePoliticaCriminalYSusPrincip-5549131.pdf

58. ZÚÑIGA, Laura. Política criminal. En: MORALES, Emma. Algunas reflexiones sobre política criminal y sus principales tendencias. *Revista Nuevo Derecho* [En línea]. Enero-junio de 2010, No. 6, p. 2. [Consultado: 04 de marzo de 2021]. Disponible en: file:///C:/Users/cash%20america/Downloads/Dialnet-AlgunasReflexionesSobrePoliticaCriminalYSusPrincip-5549131.pdf

59. MORALES, Emma. Op. Cit. p. 3

Por tal motivo, la razón metódica de la política criminal, acorde con Luzón Peña, citado por Mira, prevé las siguientes fases de actuación:

- Orientación de la creación legislativa, guiando al legislador para la creación del Derecho Penal o de nuevas instituciones jurídico penales, o incluso extrapenales como la prevención del delito;
- Orientación de la labor dogmática, orientando las categorías sistemáticas y las tendencias interpretativas según los principios propios de la política criminal; y
- Critica del Derecho vigente y propuestas, acudiendo a criterios técnicos, principios jurídicos, políticos y conocimientos empíricos de las ciencias sociales.[60]

4.1.3. Características de la política criminal.

- **Actuación Estatal:** La política criminal constituye un conjunto de estrategias establecidas por el Estado para hacer frente a la criminalidad.
- **Preventiva:** El principal fin que persigue la política criminal es la prevención del delito a través del derecho penal, instrumentos de carácter social y mecanismos jurídicos no penales.
- **Se desarrolla en Estados democráticos:** La política criminal se caracteriza por desarrollarse en Estados democráticos, teniendo como enfoque principal la prevención, el respeto de los principios y garantías estatales, y los derechos humanos y fundamentales. [61]

---

60. LUZÓN, Diego. citado por MIRA, Carlos. Manual de derecho penal, Parte General. En: MORALES, Emma. Algunas reflexiones sobre política criminal y sus principales tendencias. *Revista Nuevo Derecho* [En línea]. Enero-junio de 2010, No. 6, p. 2. [Consultado: 04 de marzo de 2021]. Disponible en: file:///C:/Users/cash%20america/Downloads/Dialnet-AlgunasReflexionesSobrePoliticaCriminalYSusPrincip-5549131.pdf

61. TAMARIT, Josep. La política criminal como disciplina empírica y valorativa [En línea]. España: UOC, 2016, p. 13 [Consultado el 04 de junio de 2021]. Disponible en: https://openaccess.uoc.edu/webapps/o2/bitstream/10609/92529/1/Pol%c3%adtica%20criminal_M%c3%b3dulo%202_%20La%20pol%c3%adtica%20criminal%20como%20disciplina%20emp%c3%adrica%20y%20valorativa.pdf

- **Axiológica:** Es decir valorativa, en donde el derecho penal expone y la política criminal cuestiona y critica. [62]
- **Instrumental**: No se limita a una dimensión valorativa, sino que materializa estrategias que permiten dar cumplimiento a sus fines. [63]
- **Diacrónica:** Estudia el pasado y proyecta cambios o reformas para los futuros sistemas de control, no preocupándose únicamente de lo actual.[64]
- **Interdisciplinar:** Se vincula con otras ciencias como el derecho penal, la criminología, la sociología, la ciencia política, entre otras.

4.1.4. Objetivo y área de investigación de la política criminal.

Como notoriamente ya lo expresó una vez Binder, el objeto en que se enfoca la política criminal son los conflictos, consistentes en las conductas ya clasificadas legalmente como delictivas, y con el fin de contrarrestarlas se promueven la elaboración de planes gubernamentales para el control de la delincuencia, aunque no exclusivamente punitivos, se concentran en aspectos de prevención, contención, resolución y tratamiento del fenómeno delictivo, en correspondencia con los principios constitucionales, los derechos fundamentales y las normas internacionales.[65]

En tal sentido, cabe destacar, que al igual que las conductas delictivas y las penas deben estar previamente fundamentadas en la Constitución, leyes secundarias y

62. SlideShare. Política criminal. [En línea] [Consultado el 04 de junio de 2021]. Disponible en: https://es.slideshare.net/fcokadir/politica-criminal

63. TAMARIT, Josep. Op. Cit. p. 11

64. SlideShare. Política criminal. [En línea] [Consultado el 04 de junio de 2021]. Disponible en: https://es.slideshare.net/fcokadir/politica-criminal

65. AMAYA, Edgardo. Bases para la discusión sobre política criminal democrática. En: FUENTES, María, et al. *Análisis de la política criminal en el salvador* [En línea]. Tesis de titulación de licenciatura en Ciencias Jurídicas. Universidad de El Salvador, 2005, p. 5 [Consultado el 03 de marzo de 2022]. Disponible en: https://ri.ues.edu.sv/id/eprint/7551/1/ANALISIS%20DE%20LA%20POLITICA%20CRIMINAL%20EN%20EL%20SALVADOR.pdf

sujetas a todos los aspectos antes indicados; así también, como ya lo expresa Binder: “la Política Criminal se encuentra autolimitada por una definición previa de los conflictos”, por lo que esta no puede depender en ningún momento de una modificación improvisada o antojadiza por motivos políticos o profundos conflictos sociales, vulnerando los derechos humanos y las garantías tanto procesales como constituciones, por dar una solución inmediata a dicha problemática, por lo que se aconseja de previo la elaboración de algún plan integral para el control de la criminalidad que ataque la base del problema, con énfasis en la prevención y contribución con la cultura de paz, para el logro de dicho fin.[66]

En resumen, según PiedeCasas, los objetivos de la Política Criminal se centran en:

- Estudiar la determinación de los fines que pretendan ser alcanzados mediante la utilización del Derecho penal;
- Sistematizar, en función de los fines y principios preestablecidos, los medios disponibles para el control de los comportamientos desviados; y
- Examinar las distintas fases del sistema penal en función de los criterios marcados en los momentos anteriores.[67]

Por su parte, en lo referente al área de investigación de la Política Criminal, se puede señalar que esta ha presentado innegable dinamismo conforme las necesidades contemporáneas de la sociedad, pasando de exclusivamente controlar la

66. FUENTES, María, et al. *Análisis de la política criminal en el salvador* [En línea]. Tesis de titulación de licenciatura en Ciencias Jurídicas. Universidad de El Salvador, 2005, pp.5-6 [Consultado el 03 de marzo de 2022]. Disponible en: https://ri.ues.edu.sv/id/eprint/7551/1/ANALISIS%20DE%20LA%20POLITICA%20CRIMINAL%20EN%20EL%20SALVADOR.pdf

67. PiedeCasas, Miguel. Lecciones del Derecho penal, parte general. En: MORALES, Emma. Algunas reflexiones sobre política criminal y sus principales tendencias. *Revista Nuevo Derecho* [En línea]. Enero-junio de 2010, No. 6, p. 2. [Consultado: 04 de marzo de 2021]. Disponible en: file:///C:/Users/cash%20america/Downloads/Dialnet-AlgunasReflexionesSobrePoliticaCriminalYSusPrincip-5549131.pdf

criminalidad mediante su estudio y preocupación, al control y reglamento de los aspectos de prevención y tratamiento de las consecuencias del delito.[68]

5. Recapitulación.

Los conceptos de Ciberdelincuencia, Criminología, Política Criminal y Control Social, definidos aquí, sustentan las bases fundamentales en que se justifica el enfoque de esta investigación.

Comprendiéndose la ciberdelincuencia como el acto que infringe la ley mediante el empleo de las tecnologías de la información y la comunicación (TIC) diferenciado entre delitos dependientes de los medios informáticos y delitos propiciados por los medios informáticos.

Cuyo tratamiento, por su complejidad y características, ha significado la readecuación de los paradigmas teóricos de la teoría del delito y de los pensamientos dogmático penales mismos.

Por lo que los conceptos de criminología, control social y política criminal vienen a desempeñar un papel esencial para la eficacia de su regulación. Por consistir la criminología en un poderoso instrumento para la prevención de delitos y conductas desviadas dentro del marco político criminal, que auxilia al Derecho Penal, por su carácter empírico y multidisciplinar, para dar respuestas que contribuyan a la convivencia humana.

Consistiendo la política criminal en el objeto que relaciona la dogmática penal y el saber criminológico, por constituir en un sector del conocimiento, entre la teoría y la práctica, basado en las estrategias, medidas y criterios tomadas por el Estado para prevenir y reaccionar frente al fenómeno criminal.

68. FUENTES, María, et al. Op. Cit. p. 7

Impactando todo esto en el control social por basarse en las reglas y principios empleadas para garantizar el orden social, que en el ámbito penal refieren al sistema de control reactivo, integral y formalizado.

CAPÍTULO II.

INCIDENCIA DE LA CRIMINOLOGÍA EN LA BÚSQUEDA DE LA EFICACIA NORMATIVA.

La eficacia es el objetivo que toda norma jurídica debe alcanzar, y también, es uno de los elementos de mayor interés para la criminología moderna como ciencia encargada del estudio del fenómeno criminal, pero también, de la normativización efectiva de las leyes penales para la adecuada prevención, persecución y sanción de los delitos.; razón por la cual se ahondará en el estudio de este componente teniendo como meta el proporcionar parámetros que den lugar a su adecuada instauración en el marco del control social penal en materia de cibercriminalidad, para lo cual se expondrán nociones generales, requisitos elementales y pautas metodológicas de evaluación con base en la criminología.

1. Eficacia de las normas jurídicas.[69]

Según la doctrina de Hans Kelsen, es posible hablar de dos tipos de eficacia normativa:

- **Eficacia Instrumental:** Se entenderá que una norma es instrumentalmente eficaz cuando al ser aplicada ésta logra los objetivos designados en el texto jurídico y, al mismo tiempo, es habitualmente obedecida por los sujetos a quienes se dirige.
- **Eficacia Simbólica:** Una norma será simbólicamente eficaz cuando su promulgación y, en algunos casos, aplicación o acatamiento, llevan al cumplimiento de unos objetivos que no se hacen explícitos en la ley, pero que

69. OSORIO, Valentina y CORREA, Laura. *La eficacia en el ordenamiento jurídico colombiano: El caso de la ley 789 de 2002* [En línea]. Trabajo de grado. Universidad EAFIT de Medellín, 2010, pp. 10-63 [Consultado el 24 de abril de 2022]. Disponible en: https://repository.eafit.edu.co/bitstream/handle/10784/12065/Valentina_CoulsonOsorio_Laura_Ram%C3%ADrezCorrea2010.pdf?sequence=2&isAllowed=y

son motivo de su creación, y diferentes a aquellos que se toman en cuenta para determinar la eficacia instrumental.

Es importante aclarar que para el tema que nos compete, solo será estudiada la eficacia instrumental, pues nuestro objetivo es el análisis del marco legal en materia de cibercriminalidad, es decir, de un conjunto de normas que sí han sido creadas para ser aplicadas y producir resultados de acuerdo a los objetivos y fines propuestos por el legislador; dicho esto, se profundizará a continuación en el estudio de esta tipología de eficacia.

1.1. Eficacia instrumental.

La eficacia instrumental se relaciona con el impacto o incidencia que tienen las normas jurídicas en la conducta humana y si la misma se adapta a los preceptos jurídicos.

Una norma que logra adecuar el comportamiento humano de sus destinatarios a los preceptos normativos, es una norma instrumentalmente eficaz.

Ahora bien, dentro de todo sistema jurídico siempre habrá algunas normas más eficaces que otras, ya sea debido, por ejemplo, a la percepción social de la misma; al igual que en los distintos países siempre habrá algunos con normas más eficaces en comparación con otros, esto debido a factores como, por ejemplo, el contexto social.

Igualmente, los resultados de un estudio de la eficacia instrumental de una ley pueden ser diferentes según el tipo de destinatario que se estudie. Pues, como bien se sabe, las normas están dirigidas tanto a órganos facultados, como a la policía, la fiscalía, los jueces, a los individuos, o a otros entes, dependiendo del tipo de norma de que se trate.

Ahora bien, la eficacia instrumental, no se configura únicamente cuando los destinatarios cumplen con lo estipulado en la ley, sino que, hay otra dimensión del derecho que se debe incluir en el análisis de ésta y es la de sus fines u objetivos.

1.1.1. Condiciones de eficacia instrumental normativa que tienen su fundamento en la criminología.

1.1.1.1. La sociabilidad.

Según la sociología moderna, la sociabilidad es la capacidad innata e inexorable del hombre de establecer vida social o en sociedad. Este término no debe confundir del de socialización; la sociabilidad estará atada a una relación innata, algo muy espontáneo, mientras que socialización se presenta como la forma en que los individuos se relacionan en busca de sus intereses. Así, la sociabilidad es "la forma lúdica de la socialización".[70]

Las relaciones sociales no son posibles sin las estructuras sociales, sin marcos de referencias como la familia, la religión, los centros laborales, los centros educativos, etc., lo que establece la existencia de varios tipos de sociabilidad de acuerdo con sus dinámicas organizacionales y culturales, convirtiéndose en un fenómeno social o hecho social que, en cualquier caso, estará mediado por reglas fuera del individuo que son interiorizadas por este con el objetivo de establecer un accionar social.[71]

Esto es lo que se conoce como control social informal, y un Derecho penal completamente desconectado del control social informal resulta de hecho inimaginable, pues la norma penal, el sistema jurídico penal y el Derecho penal como un todo, sólo tienen sentido si se les considera como la continuación de un conjunto de instituciones públicas y privadas que la propia sociedad pone a su disposición para que, en mayor o menor medida, actúen moldeando a sus iguales según ciertas características y peculiaridades con el objeto de producir un efecto de desmotivación criminal.

Así pues, la sociabilidad contribuye en gran manera a la formación de ciudadanos de bien, al sentimiento de bienestar y seguridad, a la buena salud física y metal,

70. CHAPMAN, Willian. El concepto de sociabilidad como referente del análisis histórico. *Investigación & Desarrollo* [En línea]. ENE-JUN 2015, No. 1, p. 5. [Consultado el 24 de abril de 2022]. Disponible en: https://www.redalyc.org/pdf/268/26839041001.pdf

71. Ibídem. p. 6

proporciona modelos a seguir y principalmente, apartar la mirada de la antisocialidad, es decir, de la delincuencia. Por el contrario, una deficiente sumabilidad genera más probabilidades de que los individuos actúen conforme a sus propios intereses y contrario a los de otros o al interés general.

De acuerdo a esto, la sociabilidad, es un elemento determinante para el cumplimiento habitual de las pautas jurídicas, pues verdaderamente las normas penales por sí solas son insuficientes y paradójicamente demasiado débiles para mantener el sistema de valores sobre el que descansa una sociedad; por lo que en nada servirían ni la conminación penal contenida en las mismas, ni la imposición de la pena, ni su ejecución, si no existieran previamente otros sistemas de motivación del comportamiento humano en sociedad.

Es por eso que el proceso de sociabilidad vendría siendo una condición de eficacia, un requisito que se puede predicar de todo tipo de normas, y que encuentra su fundamento en la criminología como ciencia que procura la prevención antes que la sanción, y de hecho que, las mayores garantías de éxito en orden a la prevención del delito residen fácilmente, no en el endurecimiento del control social formal, sino en su efectiva integración con el control social informal.

Ahora bien, el Estado también debe procurar su participación en los procesos de sociabilidad sirviendo como facilitador de los mismos y favoreciendo su buen funcionamiento, ya sea a través de instituciones, programas o proyectos sociales, familiares, educacionales, pedagógicos, psicológicos, culturales, emocionales, espirituales, entre otros, que contribuyan a fortalecer los lazos sociales existentes y creen nuevos antes nulos.

Estas intervenciones Estatales deben dirigirse principalmente al ámbito familiar, considerando que la familia es la principal organización social en una sociedad a través de la cual se establecen recíprocas dependencias y vínculos afectivos; encaminando a que las mismas se desenvuelvan en un ambiente seguro, de apoyo y respeto, especialmente por el bien del interés superior de los niños, niñas y adolescentes que son los que suelen sufrir las mayores consecuencias derivadas de problemas intrafamiliares, violencia doméstica, crisis de parejas, separación y

divorcio; situaciones que posteriormente –aunque no siempre— terminan contribuyendo a la antisocialidad o a la ejecución de otras acciones que si bien no involucran un acto delictivo, motivan o facilitan a su ulterior realización.

1.1.1.2. El conocimiento de las normas jurídicas.

Es necesario que los individuos de una sociedad tengan un cierto grado de conocimiento sobre las normas jurídicas.

Ello no implica que las personas deban conocer todas las normas jurídicas, pero sí que deban saber las más básicas y estar en condiciones de obtener información al respecto de las leyes que desconocen.

Si bien es cierto, nadie puede alegar ignorancia ante la ley, pues igual el carácter obligatorio de la misma la hace aplicable a razón del principio de *ignorantia iuris non excusat*[72], es razonable pensar que, si una persona no conoce una norma, no se puede esperar que modifique su conducta para satisfacer su contenido, asimismo, si se trata de una víctima, el desconocimiento conlleva fácilmente a la no denuncia, y, por lo tanto, a la impunidad, lo que consecuentemente refuerza la reincidencia delictiva.

Esta falta de conocimiento de las normas es en realidad un problema mucho más común de lo que se piensa, y que se presenta principalmente cuando se trata de normas recientes como bien podría ser el caso de las normas sobre ciberdelincuencia, que al menos en nuestro país es relativamente novedosa y en cuyo caso el conflicto de vuelve aun mayor, pues las TIC se caracterizan por sufrir modificaciones importantes de forma casi constante, de forma tal que los modos de comunicación social, de intercambio económico, de difusión de contenidos, o cualesquiera otros que se utilizan en un determinado momento, pueden ser sustituidos en muy poco tiempo por evoluciones que pueden ir desde una pequeña modificación hasta una auténtica revolución del sistema, y los bienes que hoy

72. Diccionario Jurídico de Derecho, Enciclopedia jurídica. Ignorancia de la ley. [En línea] [Consultado el 24 de abril 2022]. Disponible en: http://www.enciclopedia-juridica.com/d/ignorancia-de-la-ley/ignorancia-de-la-ley.htm

parecen intocables frente a las TIC, pueden pasar a ser susceptibles de ataque en un instante, y las soluciones jurídicas de hoy pueden llegar a ser obsoletas el día de mañana, lo que demanda de constantes actualizaciones y cambios normativos.

Otra dificultad derivada de esta falta de conocimiento es la imposibilidad de valorar la perspectiva social que se tiene de las normas, pues si hay desconocimiento, no se pueden emitir criterios o juicios de valor sobre la misma, por lo que la sociedad no podría cuestionar las leyes o refutarlas.

Esta perspectiva social de las normas jurídicas es uno de los elementos de mayor relevancia para la criminología moderna, de hecho, muchos estudiosos de la materia han centrado su atención en recoger las impresiones de los ciudadanos sobre las normas, leyes, y la manera de hacerlas cumplir, esto mediante encuestas, seminarios, conferencias y la difusión sistemática de los resultados de sus investigaciones, todo con el fin de comprender el nivel de aprobación social de una norma, información que da lugar a que las autoridades visualicen qué áreas deben mejorar, cuáles son las razones o los beneficios que eso acarrearía y consecuentemente, ejercer una influencia en la administración de justicia y las autoridades judiciales.

Sin embrago, no se puede recoger la perspectiva social de una norma si la sociedad es ignorante sobre lo misma o desconoce incluso de su existencia.

Es precisamente por estas razones que el Estado debe buscar que sus ciudadanos cuenten con la mayor información de los preceptos jurídicos para que los incluyan dentro de sus grupos, los den a conocer a sus miembros y, de esta manera refuercen su aplicación; no solo a través de mecanismos de publicidad en Diarios Oficiales, sino por medio de la realización de programas, proyectos o campañas que permitan el aumento del conocimiento de las normas y, consecuentemente, reduzcan la discriminación en su acceso y uso, sobre todo en las clases más bajas que son las que menos conocimiento tienen de sus derechos.

1.1.1.3. Aceptación de las normas jurídicas.

La aceptación o no de las normas jurídicas tiene relación con la percepción social que se tenga de las mismas, ya sea por su legitimidad o por los juicios de valores que la envuelvan.

Así pues, la conformidad o aceptación de las normas por parte de sus destinatarios implica que estos cumplirán lo que se ordena puesto que han internalizado el comportamiento preceptuado y han decidido actuar de acuerdo a él libremente y por su propia voluntad. Dicho fenómeno puede ser espontáneo o reflexivo.[73]

- **Espontáneo:** Ocurre cuando la persona cree que la conducta establecida por la regla es buena, lo que lo motiva a obedecerla, incluso en contra de su propio interés personal, porque es bueno para otras personas o para las personas en general. Esta creencia se basa, principalmente, en considerar que la norma tiene una justificación moral, religiosa, ética, debido a su utilidad, o por ser perciba como justa; la justicia no es simplemente la idea de igualdad aplicada a las relaciones del hombre con sus semejantes, claro que alude a la idea de igualdad, pero también se refiere a la idea de armonía, la búsqueda del bien común y la felicidad de todos los individuos en base a la justa razón. Entonces, al hablar de la justicia de la norma, se hace referencia a la correspondencia o no de esos valores superiores o finales que deben inspiran determinado orden jurídico.
- **Reflexivo:** Proviene de un razonamiento que hace la persona sobre por qué debe asumir el derecho. Implica que las personas obedezcan una norma, no por interés propio, confianza en el legislador o en una convicción del valor sustantivo de la ley, sino porque la misma está dotada de obligatoriedad, esto es, de legitimidad; la cual implica que la norma sea obedecida sin que medie el recurso del monopolio de la ley, pues se reconoce lo que la norma representa y el poder que simboliza.

Con todo lo anterior, cuando una norma es percibida positivamente por la sociedad, es masivamente obedecida, no siendo necesaria la aplicación de una sanción, salvo

73. OSORIO, Valentina y CORREA, Laura. Op. Cit. p. 23

casos puntuales, dicho a la inversa, el cumplimiento de una norma jurídica de manera habitual suele ser prueba de que es aceptada o percibida de forma positiva.

1.1.1.4. La motivación de las normas jurídicas.

Las leyes, requieren de medios de estimulación que motiven a sus destinatarios a cumplirlas, estos medios son las denominadas consecuencias jurídicas, que pueden ser negativas o positivas.

- **Negativas:** Son las que más se conocen y se aplican típicamente en el derecho penal consistente en una pena, una medida de seguridad, una consecuencia accesoria o en la responsabilidad civil derivada del delito, que se impone cuando se verifican los requisitos del supuesto de hecho de la norma, llamado *precepto*, *presupuesto* o *norma primaria*.[74]
- **Positivas:** Son las que se utilizan para hacer que las personas actúen de una determinada manera considerada útil, sin tener que obligarlas por medio de la fuerza, y suelen aplicarse en materia tributaria o empresarial.[75]

Aunque las consecuencias positivas y negativas son importantes fuentes de motivación para los destinatarios de las normas, éstas deben cumplir con ciertos factores de aplicación social.

Como, por ejemplo, el grado de certeza de su aplicación, el alcance de los medios y recursos empleados para su eficacia, la condición de sanciones, la percepción del riesgo de la efectividad de la sanción, entre otros.

Sin embargo, el elemento de mayor relevancia es la ejecución efectiva de los mismos, pues si las consecuencias no son aplicadas, no tendrán ningún efecto instrumental sobre los destinatarios.

---

74. Diccionario Prehispánico del Español Jurídico. Consecuencia jurídica del delito. [En línea] [Consultado el 24 de abril de 2022]. Disponible en:https://dpej.rae.es/lema/consecuencia-jur%C3%ADdica-del-delito

75. OSORIO, Valentina y CORREA, Laura. Op. Cit. p. 26

Para que las consecuencias jurídicas sean debidamente aplicadas, se demanda la existencia de:

- **Recursos humanos:** Operadores de justicia altamente capacitados que actúen bajo la previsión de los principios generales del derecho y de aquellos que rigen las normas específicas de la materia.
- **Recursos técnicos:** Herramientas e instrumentos que le permitan a los operadores ejecutar y dar cumplimiento a la norma en el modo y tiempo establecidos
- **Recursos económicos:** Recursos monetarios para la adquisición de recursos técnicos y, además, para la inversión en capacitaciones, aprendizaje continuo, formación, actualización, entre otras cuestiones.

En el campo de la ciberdelincuencia se requieren de conocimientos especializados que permitan a los operadores de justicia comprender los aspectos conductuales especiales del ciberdelito para luego proceder a implantar procesos judiciales dinámicos y ajustados a la nueva realidad tecnológica.

Este conocimiento debe estar complementado con el saber criminológico, pues solo de esa manera es posible la construcción de políticas de persecución penal efectivas contra el ciberdelito enfocadas en la víctima y el victimario.

Con todo esto, si la sociedad observa que un buen número de preceptos no son aplicados, no obedecerá las normas, al menos no, si no las acepta como adecuadas o válidas. En cambio, si el Estado hace cumplir la mayoría de las normas, las personas pensarán que no pueden dejar de someterse a ellas pues el Estado es activo en su control y es probable que los sancione por su actuación ilegal o les dé el premio correspondiente por el cumplimiento del precepto.

Para el caso que nos compete, que es la materia penal, se ha observado que la imposición de una sanción –tal como se predicó en el apartado sobre sociabilidad— se lleva a cabo primariamente a nivel social, en el seno de la familia o de grupos sociales más o menos amplios.

Sin embargo, la función motivadora emanada de esas instancias informales de control social sería ineficaz si no fuera confirmada y asegurada, en última instancia, por la función motivadora de la norma penal; pues la sociedad, a la par de conflictiva, necesita muchas veces de un orden más coactivo, más preciso y vigoroso que le garantice un cierto grado de respeto y acatamiento a sus normas.

Importante es destacar que, para que las sanciones generan motivación en sus destinatarios no requieren precisamente ser altamente represivas, pues ya la criminología afirma que a los infractores les importa más el grado de efectividad de la aplicación de la sanción, antes que la gravedad de la misma.

Estudios criminológicos como el de Paz Ciudadana de 2018 ha demostrado que no hay evidencia robusta que indique que el aumento de la severidad de las penas sirva para mejorar la disuasión de la delincuencia, citando estudios internacionales de 2003, 2006, 2008 y 2011. Siguiendo esta misma idea, Paz Ciudadana cita un análisis realizado en Alemania el 2009, basado en la revisión de 700 estudios sobre los efectos de la disuasión, que concluyó que la disuasión tiene efectos, pero que estos no son estadísticamente significativos, encontrando que la disuasión ocurre más usualmente en los casos de infracciones administrativas más que en los delitos.[76]

Es por eso también que se recomienda optar por la aplicación de las penas privativas de libertad únicamente en los casos estrictamente necesarios; optando en cambio por otras de carácter comunitario, cuestión que se explica más a detalle en el apartado sobre política criminal.

Con esto no abogamos por las penas como medios efectivos contra la criminalidad—pues la misma criminología afirma su ineficacia— sino únicamente como un medio de aseguramiento efectivo cuando las instancias de control informal

76. Biblioteca del Congreso Nacional de Chile. Efectos del agravamiento de las penas frente a la comisión de delitos. [En línea] [Consultado el 20 de julio de 2022]. Disponible en: https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/24913/1/Efectos_del_agravamiento_de_las_penas_frente_a_la_comision_de_delitos.pdf

resulten ineficaces; pues si el control informal falla y el control formal es ineficaz, todo el sistema queda inoperante y el orden social no sería más que una ficción.

1.1.1.5. La aplicación de una adecuada técnica legislativa.

Es muy común escuchar decir que “La ley No. XX es mala”, sin embargo, dicha expresión no indica con precisión si, a juicio del dicente, se trata de un texto defectuosamente escrito o si la decisión política contenida en ese texto es contraria al bien común. Pues en efecto, no es lo mismo una norma con una defectuosa técnica legislativa; que una que no pasa el test de justicia impuesto por la sociedad.

En tal sentido, definir apropiadamente la significación de la acentuación de técnica legislativa, a fin de distinguirla de otras terminologías similares, pero con distinto contenido, es de gran interés.

Así pues, son muchas las determinaciones conceptuales existentes en torno a la técnica legislativa, por lo que, algunos la ubican en el procedimiento total de elaboración de una norma, y otros, en el contenido normativo de la misma; no obstante, a fin de evitar confusión y sin intención de ofrecer una definición unilateral, definiremos para este estudio a la técnica legislativa como:

Aquella actividad no precisamente ejecutada por el legislador –pues puede ser realizada por un técnico especial— a través de la cual se transcribe o traduce a un texto escrito la decisión política del legislador. Esta traducción debe cumplir tres requisitos básicos:

- **Coherencia con el resto del ordenamiento jurídico:** Debe mantenerse la coherencia entre la norma que se propone y el resto de la normativa vigente.
- **Fidelidad de la decisión política que motivó al legislador:** La decisión política no debe ser alterada, sino claramente definida. Por supuesto, si la decisión política no es clara, el cumplimiento de este requisito se transformará en algo imposible

- **Análoga interpretación para todos los lectores:** El texto debe ser interpretado de la misma manera por cualquier lector, condición sine qua non para garantizar los derechos elementales de seguridad jurídica y de igualdad ante la ley.

Con todo esto, y siguiendo las enseñanzas de Fermín Ubertone, la Técnica Legislativa es el arte de elaborar textos normativos sin defectos, o con la menor cantidad posible de defectos.[77]

Una norma correcta y sin defectos es aquella que es clara, precisa y concisa. Es decir, aquella que transmite un mensaje indudable, de fácil comprensión y sin ser más extensa de lo necesario; lo que involucra la adecuada implementación de reglas de redacción, términos, sintaxis, modo y tiempos verbales, ortografía; así como una estructuración sistemática de todo el texto jurídico.

Una norma que no aprecia estos elementos, es una norma que carece de certeza y cognoscibilidad, que genera confusión y, por lo tanto, inseguridad jurídica e ineficacia instrumental.

Así pues, y atendiendo al típico dicho mencionado al inicio, cuando una norma esta deficientemente redactada implica que no se hizo uso de una apropiada técnica legislativa; mientras que, si la norma no pasa el test de justicia impuesto por la sociedad significa que, muy probablemente, la decisión política tomada por el legislador fue errada, lo que pertenece a la dimensión de política legislativa, la cual indica los motivos que justifican al legislador a la promulgación de una norma, motivos que deberán basarse en un profundo razonamiento y análisis de los elementos en juego a fin de que dicha decisión política sea en efecto las más acertada.

77. PÉREZ, Héctor. *Manual de Técnica Legislativa*. [En línea] Buenos Aires: Konrad Adenauer Stiftung, 2007, pp. 18-19. ISBN 978-987-1285-07-5 [Consultado el 20 de julio de 2022]. Disponible en: https://www.kas.de/c/document_library/get_file?uuid=591625b8-e7d7-77d2-f52b-a340e36d83ae&groupId=287460

1.1.1.6. Otras condiciones de eficacia específicas para la materia ciberdelictual.

- Utilizar un lenguaje neutral en las normas.
- Utilizar disposiciones vigentes de derecho nacional e internacional.
- Promulgar legislación penal relativa específicamente a la ciberdelincuencia.
- Asegurar la protección de la confidencialidad, integridad y disponibilidad de las redes de computadoras y los datos informáticos.
- Armonizar la tipificación de la los ciberdelitos en el plano internacional.
- Evitar tipificar como delitos una amplia gama de actividades que puedan significar una vulneración a bienes jurídicos.
- Aprobar y aplicar marcos jurídicos nacionales relativos a las pruebas digitales.
- Evaluar constantemente las nuevas tendencias de ciberdelincuencia.

2. Evaluación de los factores que afectan la eficacia de las normas jurídicas:

Comprendidas las generalidades relativas a la eficacia instrumental, es menester definir el proceso a través del cual será posible su estudio, para lo cual resulta indispensable verificar el cumplimiento de las condiciones anteriormente estudiadas, lo que servirá como indicador de la eficacia o ineficacia de las normas, y al mismo tiempo, indicará los sectores que impiden resultados íntegramente positivos.

2.1. Proceso de evaluación legislativa:

En la doctrina es posible identificar diversos procesos para evaluar una norma, los cuales suelen variar en dependencia del enfoque, fin o momento de evaluación.

Sin embargo, dado los elementos de interés de esta investigación, la arquitectura que compone al proceso *ex post* lo hace el más apropiado para valorar la eficacia de las normas.

El proceso *ex post* hace referencia a la evaluación de aquellas normas que ya se encuentra en vigor y ha sido definido como aquel que estudia los efectos de la ley para establecer relaciones de causalidad útiles para el legislador como proceso de aprendizaje continuo, en el que se permite asegurar la capacidad del legislador de dar respuesta a la realidad social.[78]

A través de este proceso se busca, principalmente:

- Determinar si el marco regulatorio en vigor alcanzó los objetivos deseados.
- Si la aplicación de la ley o la regulación fue lo suficientemente eficaz.
- En qué medida cualquier impacto esperado o no de la intervención regulatoria se abordó de manera adecuada en el momento de concebir el instrumento normativo, pues a menudo no es sino hasta después de su implementación que es posible evaluar plenamente las implicaciones de una ley, incluyendo sus costos, la carga regulatoria que impone y su impacto directo e indirecto, por no mencionar cualquier otra consecuencia no prevista.
- Valorar si las previsiones resultantes del momento ex ante se han cumplido o no, considerando que la evaluación amerita repensar la forma en la que las normas se conciben y diseñan.

En tal sentido, entre las ventajas que se observan de evaluar una ley ya en vigor se encuentran las siguientes:

- Determinar si la ley fue capaz de cumplir con sus propósitos, lo que tendría un beneficio adicional para los órganos legislativos, en la medida en que podría redituar en el reconocimiento a una adecuada labor legislativa.
- Advertir áreas de oportunidad, sentando así las bases para una eventual reforma legislativa.
- Depurar el ordenamiento jurídico y, por tanto, eliminar aquellas normas que han quedado obsoletas al amparo de un cambio de las circunstancias o contextos en los que se aprobó.

78. JÄÄSKELÄINEN, Federico. Op. Cit. p. 150

Con todo esto, el proceso *ex post* se integra de tres elementos básicos, considerando que no se instituye un deber de evaluación sin sujeción a plazo ni a procedimiento alguno:

- **Subjetivo: Órgano o institución encargada de la evaluación:**

La institucionalización para la evaluación normativa *ex post* se puede llevar a cabo por medio de cualquiera de las siguientes maneras:

  - Creando un órgano de evaluación *ad hoc.* El termino *ad hoc* se emplea como locución adjetiva con el sentido de 'adecuado, apropiado, dispuesto especialmente para un fin.[79]
  - Bajo el mandato del Poder Legislativo o Poder Ejecutivo.
  - Atribuyendo dicha función a un órgano del Poder Legislativo o del Poder Ejecutivo.

Por lo general se recomienda hacer residir dicha función en el Poder Ejecutivo, dado que al Gobierno y a la Administración Pública les corresponde la ejecución de las leyes y es por tanto quien puede verificar más fácilmente los problemas que plantea su cumplimiento o si resultan eficaces para los fines que persiguen.

No obstante, resulta más apropiado delegar dicha responsabilidad tanto al Poder Ejecutivo encargado de la aplicación de las normas, como al Poder Legislativo encargado de dictarla; siempre bajo la supervisión de una autoridad externa independiente del Gobierno cuya objetividad esté suficientemente asegurada.

En cualquier caso, resulta crucial integrar un equipo de profesionistas con credenciales diversas para que elaboren metodologías y herramientas para llevar a cabo procesos de análisis, como, por ejemplo: economistas, estadísticos, especialistas legales, especialista en políticas públicas, incluidos personal de apoyo.

79. Diccionario panhispánico de dudas. Ad hoc. [En línea] [Consultado el 28 de mayo de 2022]. Disponible en: https://www.rae.es/dpd/ad%20hoc

Al mismo tiempo, la institucionalidad debe contar con recursos financieros disponibles para realizar el estudio y facilitar así una toma de decisiones basada en evidencias.

Ahora bien, durante la designación de la institucionalización es menester también el establecimiento claro de las atribuciones de los encargados del proceso de evaluación, el compromiso político por parte de los evaluadores, la forma en que interactuaran con otros órganos estatales y no estatales, la forma de escoger leyes para su análisis, mecanismos y medios para difundir los resultados del proceso de estudio, entre otras cuestiones que garanticen una fortaleza institucional bien definida, que, de ser posible, sean definidas en instrumentos legales.

- **Objetivo: Procedimiento a través del cual se llevará a cabo la evaluación:**

Una vez que se tiene un sistema estructuralmente adecuado y una institucionalización definida, se procede a la labor de evaluación, la cual puede desarrollarse en tres etapas:

  - Análisis teórico.
  - Estudio de campo.
  - Informe final.

El procedimiento de evaluación legislativa *ex post* debe desarrollarse de acuerdo con una metodología y fines previamente preestablecidos y multidisciplinares que no olviden los compromisos políticos establecidos en la elaboración de la norma, ni el hecho de que la evaluación no suple el marco de decisión política, sino que lo complementa, pudiendo reforzarlo o afianzarlo.

Siguiendo con esta idea, la evaluación *ex post* debe basarse en un análisis tanto cuantitativo como cualitativo. Para medir plenamente los efectos de una ley, los evaluadores *ex post* deberían basarse en estadísticas, encuestas, informes de expertos, estudios, etc.:

  - Las estadísticas son una fuente importante de análisis cuantitativo para las instituciones públicas, ya que ayudan a medir cómo se lleva a cabo la

implementación. A través de este enfoque puede estudiarse la aplicación efectiva de las consecuencias jurídicas negativas o bien el nivel de conocimiento de las normas.

- Las encuestas pueden ser una herramienta eficaz para una evaluación cualitativa del impacto social de una reforma legislativa: mediante la realización de encuestas, el evaluador podrá identificar las creencias comunes de los usuarios finales de la ley.

Pese a lo ya señalado, los pasos que habrán de seguirse durante la evaluación, así como los mecanismos o herramientas que serán utilizadas, deberán ser definidas de previo por el órgano designado para tal fin o bien por el Poder Legislativo, incluyendo los fines y objetivos que regirán cada etapa investigativa.

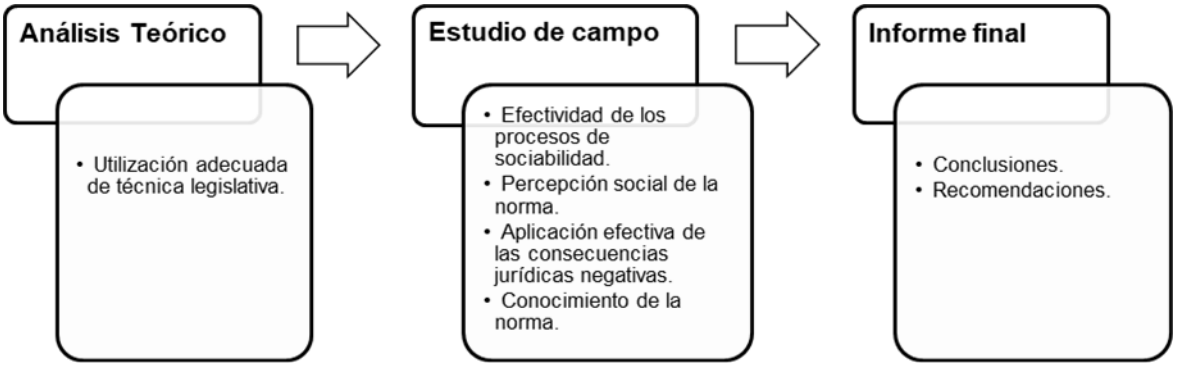
Con todo esto, las directrices y recomendaciones presentadas en este apartado son simples ejes de orientación sobre cómo puede estructurarse el procedimiento de evaluación; por lo que, y con este mismo fin, se presentan también algunas pautas metodológicas ofrecidas por la criminología, las cuales serán desarrolladas en el siguiente numeral.

En cualquiera de los casos, una vez finalizado el procedimiento de evaluación, se deberá presentar un informe detallado con la exposición de resultados y recomendaciones en torno a los objetivos específicos previamente definidos. Estos resultamos podrán versar, por ejemplo, sobre cualquier dificultad legal o de redacción específica que haya sido asunto de preocupación pública.

Así mismo es importante que los resultados de los informes sean accesibles a todo el público a fin de garantizar la participación ciudadana, esto a través de la publicidad, por diversos medios, de los informes en un lenguaje sencillo y formato claro, que incluyan –de ser posible—, glosarios de términos o guías que faciliten la comprensión de los mismos.

En el mismo sentido, se debe procurar, no solo el conocimiento de la sociedad, sino también su participación por medio del diseño de procedimientos a través de los cuales puedan incorporar sus inquietudes o realizar consultas.

Gráfico 1. *Procedimiento de evaluación legislativa ex post.* En este gráfico se muestran las etapas procedimentales de la evaluación ex post, incluyendo los elementos que deberán configurar cada una de ellas según las condiciones de eficacia instrumental.



Fuente: Elaboración propia

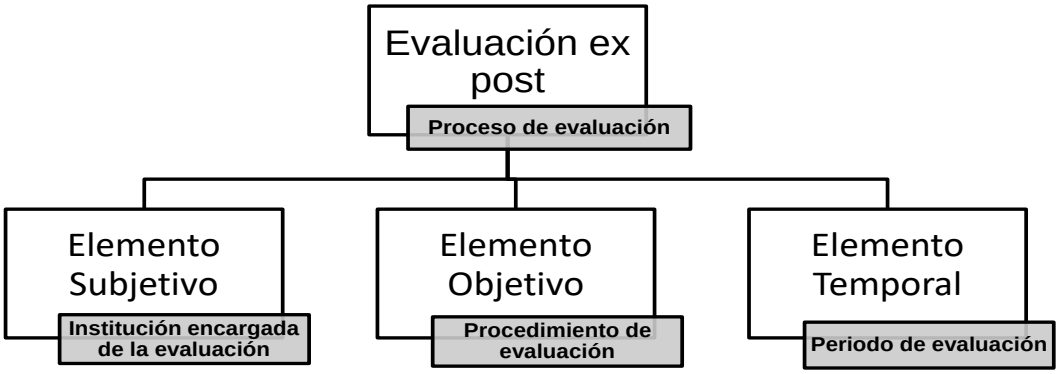
- **Temporal: Periodo general y, en su caso, específico en el que debe cumplirse con la evaluación.**

La temporalidad y el momento en que se presentará el informe depende en gran manera del tipo de norma, de la complejidad de la misma, del fin que se busca, de los sujetos que intervengan en el análisis, entre otros factores. Aunque establecer un tiempo estándar sería lo más recomendable para evitar que el proceso sea innecesariamente extenso.

En todo caso, la previsión de deber de revisión de la legislación puede, a su vez, expresarse de manera periódica, sometiendo toda la legislación a un proceso de revisión tras el transcurso de un periodo de tiempo específico (dos, cinco o diez años, por ejemplo), o valorando determinadas materias o ámbitos de regulación en una revisión periódica preceptiva; proceso que puede incluirse incluso dentro de las mismas normas jurídicas, ejemplo de esto es la reciente Ley 39/2015 de España, de 2 de octubre, la cual señala en su preámbulo que: *…en aras de una mayor*

seguridad jurídica, y la predictibilidad del ordenamiento, se apuesta por mejorar la planificación normativa ex ante … Al mismo tiempo, se fortalece la evaluación ex post, puesto que junto con el deber de revisar de forma continua la adaptación de la normativa a los principios de buena regulación, se impone la obligación de evaluar periódicamente la aplicación de las normas en vigor, con el objeto de comprobar si han cumplido los objetivos perseguidos y si el coste y cargas derivados de ellas estaba justificado y adecuadamente valorado…[80]

Gráfico 2. *Proceso de evaluación legislativa ex post.* En este gráfico se evidencian los tres elementos configurativos del proceso de evaluación *ex post*.



Fuente: Elaboración propia

80. Administración General del Estado. *Procedimiento Administrativo Común Régimen Jurídico del Sector Público* [En línea]. España: Editorial BOE, 2022, pp. 37. ISBN: 978-84-340-2259-1 [Consultado el 20 de julio de 2022]. Disponible en: https://www.boe.es/biblioteca_juridica/abrir_pdf.php?id=PUB-PB-2022-140

- **Modelo de evaluación *ex post*: Chile: [81]**

A fin de establecer mecanismos sistemáticos de evaluación legislativa, el Congreso chileno creó el Departamento de Evaluación de la Ley el 21 de diciembre de 2010. El Departamento fue creado por acuerdo de la Comisión de Régimen Interno, Administración y Reglamento. El acuerdo se comunicó por medio de la Nota Oficial número 381 de la Presidencia de la Cámara de Diputados. El acuerdo fue ratificado por medio de la Resolución No. 57 del 27 de enero de 2011, firmada por el secretario general de la Cámara de Diputados.

  - **Las principales responsabilidades de este Departamento son las siguientes:**
    - Evaluar las normas legales aprobadas por el Congreso Nacional en coordinación con el secretario de la Comisión a cargo. La evaluación se realiza con base en la eficacia de la ley y su influencia sobre la sociedad. El Departamento podrá proponer medidas correctivas para mejorar la implementación de la ley evaluada.
    - Crear y mantener una red de organizaciones sociales interesadas en participar en el proceso de evaluación.
    - Informar al secretario general por medio de la Comisión de Régimen Interno, Administración y Reglamento acerca de los resultados de la evaluación.
    - Sugerir enmiendas a la legislación vigente de ser necesario.

El proceso actual prevé principalmente la elaboración de un informe final que incluya un análisis de los impactos de la implementación de la ley y la percepción que los ciudadanos tienen de la misma.

81. OCDE. *La Evaluación de Leyes y Regulaciones: El Caso de la Cámara de Diputados de Chile* [En línea]. París: OCDE, 2012, pp. 50-67 ISBN: 978-92-64-17636-2 [Consultado el 24 de julio de 2022]. Disponible en: https://read.oecd-ilibrary.org/governance/la-evaluacion-de-leyes-y-regulaciones_9789264176362-es

Los tipos de impactos analizados, en dependencia del tipo de norma de que se trate son: económicos, financieros, sociales, culturales, ambientales, institucionales y legales.

- **El análisis de la ley tiene los siguientes objetivos:**
  - Determinar el grado de cumplimiento de los objetivos esperados cuando se aprobó la ley.
  - Identificar las externalidades, el impacto y las consecuencias indeseadas cuando el Congreso estaba legislando.
  - Conocer la percepción de los ciudadanos acerca de la ley y su implementación.
  - Proponer medidas correctivas para la ley y su implementación.

El primer proceso de evaluación realizado por esta institucionalización fue en el año 2011 sobre la ley 20.413 sobre donación de órganos, cuyos resultados fueron publicados en la página oficial de Evaluación de Leyes de la Cámara de Diputados De Chile[82], informe que demostró que no se había tomado en consideración una serie de temas cuando se discutió la ley por primera vez, como la falta de una política nacional acerca del trasplante de órganos donados que podría incluir temas relacionados con la educación, el financiamiento y la transparencia del sistema en términos del manejo de la información, así como la falta de infraestructura y recursos humanos dedicados a garantizar que se encuentre vigente una política de donación.

82. Cámara de diputados de Chile. Evaluación de la Ley. [En línea] [Consultado el 24 de julio de 2022]. Disponible en: https://www.evaluaciondelaley.cl/leyes-evaluadas/

2.2. Algunas pautas metodológicas dadas por la criminología para la evaluación legislativa.[83]

La criminología resalta la necesidad de adquirir suficiente información acerca del fenómeno criminal previo a la relación de una evaluación legislativa, información que podrá versar en:

- Tipologías de los delitos.
- Perfiles de detección del crimen.
- Perfiles del delincuente.
- Perfiles de víctimas.
- Datos de victimización.
- Otros cuerpos normativos de países con similares contextos socio-criminales. (Realizar estudios comparados)

La información recolectada deberá versar asimismo sobre la realidad criminal del entorno estudiado –con el propósito de ser convertida en estadística que posteriormente sea sinterizada— ya sea sobre:

- Delitos más relevantes.
- Frecuencia de los delitos.
- Proporción en que se resuelven los delitos denunciados.
- Impacto sobre el desempeño económico, social, laboral, cultural, etc.

Esta información puede ser recolectada a través de diversas técnicas e instrumentos, pero siempre provenir de diversas fuentes y no únicamente de fuentes oficiales o judiciales, esto debido a que son, no solo insuficientes, sino también engañosas, ya que; por un lado, recogen solamente información de delitos denunciados, es decir, delitos conocidos y juzgados, sin tomar en cuenta aquellos

83. RUBIO, Mauricio. *Evaluación de las leyes: Lecciones de la criminología.* Revista de economía institucional [En línea]. JUL-DIC 2008, No. 19, pp. 153-157 [Consultado el 11 de marzo de 2022]. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=2777479

delitos cometidos que no se conocen oficialmente; y, por otro lado, muchas veces no se trata de la información que no llega a las autoridad judiciales, sino de la información que las misma autoridades llegan a excluir de los informes.

Por esta razón la información debe provenir de diversas fuentes, con el objetivo de que los resultados sean confiables, verídicos y menos sujetos a discusión.

Por otro lado, la criminología enseña que la evaluación de las leyes debe realizarse desde un enfoque micro, es decir, desagregado, bajo objetivos debidamente definidos y delimitados que eviten que las conclusiones a las que se lleguen o las recomendaciones que se propongan resulten demasiado globales y ambiguas que solo dificulten su proceso de aplicación.

Para este caso es recomendable que cada uno de las condiciones estudiadas sean valoradas una a una (ejecutar diversos procesos de evaluación por cada elemento que pretenda ser valorado), pues si bien es cierto todo crimen tiene su origen en múltiples causas las cuales se entrelazan y confunden –pues de hecho que la multiplicidad es la regla general en los fenómenos humanos a los cuales casi nunca se les puede atribuir una causa única no relacionada con otras— cada una de ellas, por las necesidades del pensamiento y la palabra, se deben investigar por separado.

En el mismo sentido se recomienda centrar la atención en el análisis de los conflictos concretos y específicos, es decir, en asuntos determinados y delimitados, considerando siempre la población, el territorio, el tiempo, el fin que se busca y la constancia de las evaluaciones.

Así, los estudios o evaluaciones que toman en cuenta estos parámetros sobresalen por varios aspectos:

- Son útiles para contrastar aquellas ideas que no pasaron la prueba de datos y que, de no ser por el estudio, habrían inspirado reformas inadecuadas.
- Definen sus propias variables concretas y susceptibles de medición y comprobación.
- Generan sus propios datos y hacen explicita la metodología para recogerlos.

- El informe puede ser entendido por el público en general y no únicamente por especialistas.
- Permiten una interacción entre la teoría y la práctica.

Este esfuerzo puntual, lento, y hasta artesanal y sin duda tortuoso de recoger información, ya sea a través de expedientes judiciales o encuestas, es, sin embargo, la alternativa más prometedora, pues permite entender las reacciones de los usuarios del sistema judicial y de los criminales ante las leyes, lo que a su vez permite evaluar la eficacia del sistema operativo en general, las consecuencias derivadas de las respuestas judiciales y dan lugar a la formulación de políticas relevantes y realistas.

3. Recapitulación.

La eficacia normativa es una condición que debe predicarse de toda norma jurídica, máxime una norma de derecho penal, pues su objetivo es que las mismas produzcan los efectos jurídicos para los cuales fueron creadas.

Para que esta eficacia se presente es necesario del cumplimiento de una serie de condiciones, estas son: sociabilidad, conocimiento, motivación, aceptación y aplicación de una depurada técnica legislativa; en el caso específico de las normas sobre ciberdelitos, se amerita, además, de condiciones que permitan el buen desarrollo de la cooperación internacional, como: la armonización de las normas sustantivas, el uso de disposiciones vigentes de derecho internacional, la valoración de tendencias actuales de ciberdelincuencia, utilización de lenguaje neutral; todos elementos que encuentran su fundamento directa o indirectamente en la ciencia criminológica.

Con todo esto, la valoración de la eficacia de las normas jurídicas es una actuación de la cual el Estado no puede desprenderse, siendo los procesos de evaluación legislativa la alternativa más prometedora para este fin siempre que se realice bajo el seguimiento de lineamientos criminológicos, a través de los cuales es posible identificar exitosamente las deficiencias que perturban la observancia debida de las normas y procurar así la funcionalidad de la mismas, es decir, su efectiva

instrumentalización y producción de efectos deseados con el menor impacto negativo.

CAPÍTULO III.

RÉGIMEN LEGISLATIVO ADOPTADO POR NICARAGUA, COSTA RICA Y EL SALVADOR EN MATERIA DE CIBERDELINCUENCIA.

Toda sociedad necesita de una disciplina coercitiva que garantice la coherencia interna de sus miembros, he ahí el surgimiento de las normas jurídicas como control social formal, siendo este actualmente el campo de mayor interés para la criminología la cual ha desplazado en los últimos cuarenta años una buena parte de sus investigaciones a este terreno de enfrentamiento al acto criminal.

En ese contexto, y con el objetivo de reforzar este control formal en el marco de la ciberdelincuencia en nuestro país a través de conocimientos criminológicos, se expondrá el régimen legislativo nacional e internacional adoptado en Nicaragua, complementado con un estudio comparativo, esto considerando que la lucha contra la ciberdelincuencia requiere normas que permitan la prevención, persecución y sanción de delitos cometidos incluso fuera de las fronteras nacionales.

1. Regulación jurídica nacional.

1.1. Nicaragua.

1.1.1. Constitución Política.[84]

La Constitución Política de la república de Nicaragua con sus reformas incorporadas establece en su título IV referente a los derechos, deberes y garantías del pueblo Nicaragüense el derecho a la libertad individual, a la vida privada, el acceso a la información, a la seguridad, a la igualdad de protección, al respeto de su integridad física y psíquica, a la libertad de conciencia y pensamiento, sea esta expresada

84. Nicaragua. Constitución Política de la República de Nicaragua con reformas incorporadas. *La Gaceta - Diario Oficial*, del 18 de febrero de 2014, No. 32. Disponible en: https://www.asamblea.gob.ni/assets/constitucion.pdf

privada o públicamente, individual o colectiva, en forma oral, escrita o por cualquier otro medio.

Siendo más que clara nuestra carta magna, en lo que respecta al derecho a la inviolabilidad del domicilio, correspondencia y comunicaciones, al detallar en su art. 26 los casos en que la autoridad judicial podrá permitir su limitación, reforzando dicho derecho al dejar sin efectos a aquellos que hayan sido sustraídos ilegalmente.

Contando además con el reconocimiento y protección de derechos internacionales de corte constitucional, como apreciaremos en el art. 46 Cn, con respecto a los derechos humanos, señalando que en el territorio nacional toda persona goza del respeto, promoción y protección de los derechos consignados en la/el: Declaración Universal de los Derechos Humanos; Declaración Americana de Derechos y Deberes del Hombre; Pacto Internacional de Derechos Civiles y Políticos de la ONU; y Convención Americana de Derechos Humanos de la OEA.

Y no podemos perder de vista el valor de lo que el derecho a la información veraz significa como parte de nuestros derechos sociales, tal y como lo establecen los artos 66, 67 y 68 que parten del principio de veracidad como garantía jurídica del resguardo del derecho a la libertad de opinión y expresión como instrumento de promoción de la participación ciudadana en el ejercicio activo del derecho a la información, que también alcanza la figura del periodista y su obligación de actuar de forma diligente a fin de obtener la protección constitucional.

1.1.2. Código Penal.[85]

La Ley No. 641, mejor conocida como Código Penal de la república de Nicaragua, contiene una serie de definiciones de las acciones u omisiones tipificadas como delictivas, así como el señalamiento de las penas o medidas de seguridad aplicables para lograr la permanencia del orden social; es por ello que aunque los ciberdelitos

85. Nicaragua. Ley No. 641, "Código Penal de la República de Nicaragua". *La Gaceta - Diario Oficial*, del 5, 6, 7, 8 y 9 de mayo de 2008, No. 83, 84, 85, 86 y 87. Disponible en: http://legislacion.asamblea.gob.ni/normaweb.nsf/9e314815a08d4a6206257265005d21f9/1f5b59264a8f00f906257540005ef77e?OpenDocument

sean un tema de preocupación actual, podremos encontrar acá, desde mucho antes de la promulgación de su ley especial, la regulación de algunos delitos convencionales que también pueden cometerse mediante el empleo de las TICs, como podremos mencionar los delitos de: Acoso sexual (art.174); amenazas (art.184); chantaje (art.185); propalación (art.195); injuria (art.203); calumnia (art.202); ofensa a la memoria de un difunto (art.208); difusión no autorizada de imágenes de un difunto (art.209); estafa (art.299); etc.

Identificando únicamente seis artículos que sancionan determinadas conductas de naturaleza informática de forma directa, hoy derogados por el art. 47 de la Ley No. 1042, que en su momento significaron una limitante para la persecución del creciente fenómeno ciberdelincuencial, por limitarse su tipificación a los delitos de apertura o interceptación ilegal de comunicaciones (art.192); sustracción, desvío o destrucción de comunicaciones (art.193); captación indebida de comunicaciones ajenas (art.194); acceso y uso no autorizado de información (art.198); destrucción de registros informáticos (art.245); y uso de programas destructivos (art.246).

Consistiendo estos en un acto ilícito en el que se emplea, como medio o como fin para su comisión, de recursos informáticos. Por ello sanciona el acceso, sin derecho, a una base de datos, sistemas o red de computadoras con el propósito de dañar, alterar, obtener información… así como la intercepción, interferencia, uso, daño, alteración o destrucción de algún soporte o programa contenidos en las mismas.[86]

1.1.3. Ley 1042, ley especial de ciberdelitos.[87]

La ley especial de ciberdelitos asume por objetivo principal, a como claramente expone en su art. 1, la prevención, investigación, persecución y sanción de los

86. Justia. Preguntas y respuestas sobre delitos informáticos. [En línea] [Consultado el 10 de junio de 2022]. Disponible en: https://mexico.justia.com/derecho-penal/delitos-informaticos/preguntas-y-respuestas-sobre-delitos-informaticos/

87. Nicaragua. Ley No. 1042, “Ley Especial de Ciberdelitos”. *La Gaceta – Diario Oficial*, del 30 de octubre de 2020, Nº. 201. Disponible en:

delitos cometidos mediante las TICs, en perjuicio de las personas naturales o jurídicas, así como la protección integral de los sistemas que utilicen dichas tecnologías, su contenido y cualquiera de sus componentes.

Destacándose por el resguardo de un amplio catálogo de bienes jurídicos que podremos distinguir en tres tipos; cuya tutela completa por parte del legislador requiero de su adaptación a las nuevas necesidades de protección conforme las TICs, consistentes en la:

- **Tutela de derechos fundamentales:** La intimidad de las personas y de sus datos e información; la inviolabilidad de su correspondencia, comunicación y patrimonio; la libertad e integridad sexual; así como todos los derechos humanos de rango constitucional.
- **Tutela de bienes jurídicos de la seguridad nacional:** El ciberespacio, por ser este el medio donde se desarrollan todas las actividades virtuales; de forma que permita preservar la integridad, estabilidad y permanencia del bien común.
- **Tutela de las Telecomunicaciones:** Su seguridad, buen desarrollo, protección de datos e información que manejan las instituciones públicas.[88]

Por lo que se ubica la presente Ley como de orden público y su seguimiento de oficio, pretendiendo para ello ampliar su ámbito espacial dentro o fuera del territorio nacional, conforme el art. 2. [89]

Cabe señalar que dicha Ley consta de 48 artículos, divididos en 8 capítulos, que comprenden, según su orden: disposiciones generales, delitos relacionados con la

http://legislacion.asamblea.gob.ni/normaweb.nsf/($All)/803E7C7FBCF44D7706258611007C6D87

88. QUEZADA, Martha. Análisis jurídico de la ley 1042: "Ley especial de ciberdelitos" [En línea]. Nicaragua: Poder Judicial, 2021, pp. 25-26. [Consultado el 10 de junio de 2022]. Disponible en:https://www.poderjudicial.gob.ni/iaej/pdf/Reformas/ANALISIS%20JURIDICO%20LEY%201042.%20LEY%20ESPECIAL%20DE%20CIBERDELITOS.pdf

89. Nicaragua. Ley No. 1042, "Ley Especial de Ciberdelitos". *La Gaceta – Diario Oficial*, del 30 de octubre de 2020, No. 201. Disponible en: http://legislacion.asamblea.gob.ni/normaweb.nsf/($All)/803E7C7FBCF44D7706258611007C6D87

integridad de los sistemas informáticos, delitos informáticos, delitos informáticos relacionados con el contenido de los datos, delitos informáticos relacionados con la libertad e integridad sexual, procedimientos, medidas cautelares y procesales, cooperación internacional, y disposiciones finales; categorizándose, los delitos y sus penas, a razón de la naturaleza del delito, debido a la multiplicidad de bienes jurídicos que se pueden ver afectados en un solo delito[90], clasificándose en:

- **Capítulo II/ artos 4-11:** Delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas (los cuales sancionan tanto el acceso e intercepción ilegal, interferencia de datos y sistemas como el mal uso de dispositivos) y como método (referente a la utilización de métodos electrónicos para llegar a un resultado ilícito).
- **Capítulo III/ artos 12-15:** Delitos de fraude informático (referentes a la falsificación y fraude conceptual) y como fin (conductas criminógenas dirigidas con el objetivo de dañar).
- **Capítulos IV-V/ artos.16-35:** Delitos por su contenido (Producción, diseminación y posesión de pornografía infantil) y como medio (Comisión del delito bajo el empleo del computador como medio o símbolo).[91]

1.1.4. Ley 983, ley de justicia constitucional, énfasis en el recurso de Habeas Data.[92]

A como claramente expone, desde su preámbulo, el objeto de esta ley parte de la reglamentación de mecanismos de control, aplicables a la justicia constitucional, para el resguardo de derechos y garantías constitucionales, y el control de

90. QUEZADA, Martha. Op. Cit. p. 25

91. QUEZADA, Martha. Op. Cit. pp. 15-18

92. Nicaragua. LEY No. 983, “Ley de justicia constitucional”. *La Gaceta – Diario Oficial*, del 20 de diciembre de 2018, No. 247. Disponible en: http://legislacion.asamblea.gob.ni/normaweb.nsf/9e314815a08d4a6206257265005d21f9/1323c5d29a709b9c0625837c005a2b21?OpenDocument

constitucionalidad normativa, mediante el Recurso de: inconstitucionalidad; Exhibición Personal; Amparo y Habeas Data.

Temática de interés, por lo que centrándonos en el Habeas Data, derecho de intimidad informática, puntualizaremos sobre la acción constitucional que puede ejercer cualquier titular, sobre el control de los datos que de ellos se contiene, para su acceso, rectificación y eliminación, cuando estos les afecte, interviniendo el Estado para su tutela y protección. [93]

En tal sentido, su objetivo y finalidad, descansa en la protección de derechos constitucionales vinculados con la vida privada y familiar, honra y reputación, y la autodeterminación informativa. Por lo que el Habeas podrá emplearse para:

- **Acceder a información personal** en poder de cualquier entidad pública o privada que genere, produzca, procese o posea información personal en expedientes, estudios, dictámenes, datos estadísticos, informenes técnicos, ficheros y cualquier documento en su poder.
- **Exigir la oposición, modificación, supresión, bloqueo, inclusión, complementación, rectificación o cancelación y actualización de**: 1. Datos personales sensibles, sean físicos o electrónicos, almacenados en ficheros de datos o registros de cualquier entidad pública o privada que brinde servicio o acceso a terceros, cuando se presuma la falsedad, inexactitud, desactualización, omisión total o parcial, o ilicitud de información de que se trate. 2. Cualquier publicidad de datos personales sensibles que lesionen los derechos constitucionales.

Consistiendo, su única improcedencia, en todo acto legítimo de investigación de hechos delictivos, seguridad nacional, información pública reservada y aquellos que la legislación vigente considere.

Y en cuanto a quien podrá interponer dicho recurso, la ley establece que, se legitimará a:

93. Diccionario Panhispánico del español jurídico. habeas data. [En línea] [Consultado el 10 de junio de 2022]. Disponible en: https://dpej.rae.es/lema/habeas-data#:~:text=1.,2.

- Toda persona natural afectada
- Toda persona jurídica afectada a través de su representante legal
- Tutores y sucesores o apoderados de las personas naturales afectadas
- La procuraduría para la Defensa de los Derechos Humanos a favor del agraviado

Dirigiéndose en contra de toda persona natural o jurídica que:

- Se responsabilice de los ficheros de datos públicos o privados que haga uso indebido de los datos, donde se encuentre la información correspondiente.
- Tenga en su poder datos o documentos de cualquier naturaleza, sin estar debidamente autorizado y que haga uso indebido de estos. Esto, mediante escrito, en papel común, que en su descripción contenga los requisitos descritos en la ley.

El proceso que habrá de seguirse para este recurso de habeas data lo encontramos regulado desde el art. 32 al 41 e incluye consideraciones sobre el agotamiento de la vía administrativa, la autoridad competente, la subsanación de omisiones, y la admisión del recurso, notificación, sentencia, además de los recursos aplicables.

1.1.5. Ley 787, ley de protección de datos personales.[94]

La ley de protección de datos personales del año 2012, nace con el objetivo de asegurar el derecho a la privacidad personal y familiar y el derecho a la autodeterminación de las personas naturales y jurídicas (art. 1).

La autodeterminación implica el derecho que tiene toda persona de saber el tratamiento que se les da a sus datos personales, entendiéndose como datos personales, toda información que identifique o que haga identificable al sujeto.

Esta protección está dirigida a aquellos datos que se encuentren en registros automatizados o manuales (art. 2),los cuales deberán ser debidamente autorizados

94. Nicaragua. Ley No. 787, “ley de protección de datos personales”. *La Gaceta - Diario Oficial*, del 29 de marzo de 2012, No. 61. Disponible en: http://legislacion.asamblea.gob.ni/normaweb.nsf/9e314815a08d4a6206257265005d21f9/e5d37e9b4827fc06062579ed0076ce1d

y archivados para su licitud en la Dirección de Protección de Datos Personales en el plazo y de acuerdo al proceso determinado, (art. 4, 22, 23), debiendo obtener los datos de acuerdo a los requisitos ya establecidos por la ley (art. 5), en donde destaca el consentimiento del titular, el cual deberá ser prestado de forma expresa, por escrito, verbalmente o por medios electrónicos, no siendo necesario sólo en los casos así previstos (art. 6).

Los tipos de datos regulados en la presente ley son categorizados de la siguiente manera:

- Datos personales sensibles.
- Datos personales relativos a la salud, en los hospitales, clínicas, centros y puestos de salud, públicos y privados, y los profesionales vinculados a las ciencias de la salud (En este caso sólo podrán ser obtenidos cuando el sujeto haya acudido a ellos para recibir tratamiento, siempre que se respete el secreto profesional)
- Datos personales informáticos.
- Datos personales comerciales.

En lo que respecta al tratamiento que se les dará a los datos, la ley dispone que dependerá del consentimiento del titular, sin perjuicio de lo señalado anteriormente.

En todo caso, los datos personales sólo podrán ser tratados, cuando sean adecuados, proporcionales y necesarios en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan solicitado (art. 9).

Pudiendo el titular de los datos, en cualquier momento, solicitar que se supriman o cancelen todos los datos personales que se encuentren en redes sociales, navegadores o servidores, incluyendo las bases de datos de instituciones públicas o privadas que presten bienes y servicios o que estén destinados al envío de publicidad, promociones, ofertas y venta directa de productos, bienes y servicios, en cuyo caso el titular podrá expresar su negativa a seguir recibiendo envíos publicitarios y promocionales o, en su caso, revocar su consentimiento de una forma

clara y gratuita.(art. 10, 25, 26). Contando el titular asimismo con otros derechos relaciones (art.16-19).

Ahora bien, para asegurar la protección de estos datos personales, se establecen obligaciones a los responsables de los mismos, es decir, a aquellos encargados de decidir, conforme a la ley, sobre la finalidad y contenido de los datos personales (art. 7). Estas obligaciones se centran en el deber de comunicar o informar al titular sobre ciertos asuntos; imposición de responsabilidad en casos concretos (art. 9 y 11), prohibiciones (art. 14 y 15).

Por otro lado, por medio de esta Ley, se crea la Dirección de Protección de Datos Personales (art. 28-43) adscrita al Ministerio de Hacienda y Crédito Público, que cuenta con un director designado por la máxima autoridad administrativa de dicho ministerio y que tiene por objeto el control, supervisión y protección del tratamiento de los datos personales contenidos en ficheros de datos de naturaleza pública y privada.

Esta autoridad competente tiene la potestad de aplicar sanciones administrativas (art. 44-46) en dependencia de las infracciones en las que se incurra, las cuales son categorizadas en leves y graves (art. 47). Ante esta autoridad se agota la vía administrativa para posteriormente proceder, el titular de los datos, a hacer uso de la vía jurisdiccional, tal como lo establece la presente ley (art. 52).

Finalmente, para efectos de desarrollo y aplicación de esta Ley, se crea el Reglamento de la ley no. 787 “Ley de protección de datos personales”[95] del año 2012, el cual habla sobre el consentimiento del titular y las formas de prestarlo, las medidas de seguridad de protección de los datos, se explican a detalle los derechos del titular de los datos, el procedimiento para interponer la acción de protección de datos, entre otras cuestiones.

95. Nicaragua. Decreto ejecutivo No. 36-2012, “reglamento de la ley No. 787”. *La Gaceta - Diario Oficial*, del 19 de octubre de 2012, No. 200. Disponible en: http://legislacion.asamblea.gob.ni/normaweb.nsf/($All)/7BF684022FC4A2B406257AB70059D10F?OpenDocument

1.1.6. Ley 621, Ley de Acceso a la Información Pública.[96]

La ley de acceso a la información pública data del año 2007, y en ella se reafirma el derecho que tiene todo ciudadano, incluyendo los medios de comunicación, al acceso a la información pública como mecanismo para fortalecer la participación ciudadana, las políticas públicas, la gestión pública y por ende la gobernabilidad democrática.

El acceso a la información pública es una prerrogativa que permite a los ciudadanos conocer cualquier tipo de información generada por el Estado y su administración pública.

Esta ley será aplicada a todas las oficinas de acceso a información, incluyendo las de coordinación y la Comisión Nacional; cada una de estas entidades deberá crear una oficina a nivel interno que se encarde de recepcionar y atender las solicitudes de acceso a información a través de un sistema de organización de información y archivos.

Será responsabilidad de las entidades el establecer los mecanismos conducentes a fin de que el derecho de acceso a la información sea satisfecho en todos los casos en la medida de lo posible (art. 5-6), para lo cual deberán disponer los recursos financieros suficientes para el adecuado funcionamiento de las oficias (art. 8) y contar con los elementos de estructuración, calificación y registro detallados en la ley (art. 8-12).

Para esto, se crea la Comisión Nacional de Acceso a la Información Pública, la cual tiene como función principal velar por el adecuado cumplimiento de estas disposiciones y el bien funcionamiento de las oficinas, además de resolver los recursos de apelación en segunda instancia. Asimismo, se crea la Comisión Nacional de Acceso a la Información Pública la cual tiene entre sus funciones la

96. Nicaragua. Ley No. 621, “ley de acceso a la información pública”. *La Gaceta - Diario Oficial*, del 22 de junio de 2007, No. 118. Disponible en: http://legislacion.asamblea.gob.ni/Normaweb.nsf/($All)/675A94FF2EBFEE9106257331007476F2

formulación de propuestas de políticas públicas, promoción de capacitaciones, de acuerdos de cooperación, entre otras cosas (art. 14).

Ahora bien, a efectos de la información que podrá ser o no de acceso público, la ley diferencia entre información reservada y las de libre acceso.

La información reservada será aquella expresamente clasificada como tal mediante acuerdo del titular de cada entidad, al aplicar los criterios señalados en la ley (art. 15). Por su parte, la información de libre acceso será toda aquella no calificada como reservada (art. 16); dentro de esta información se encuentra también aquella que debe ser difundida al público de oficio por las entidades públicas y privadas, información que deberá actualizarse periódicamente (art. 20-25)

En lo que respecta al procedimiento para acceder a la información pública, la ley señala que podrá hacerse de forma gratuita directamente ante la entidad correspondiente a través de una solicitud, ya sea verbal o escrita o por algún medio eléctrico de ser posible. La solicitud escrita deberá contener los datos descritos en la ley (art. 27) y de no ser así, o en caso de que la autoridad no sea la competente o en todo caso la solicitud no sea clara, la entidad deberá hacérselo saber por escrito al solicitante, en un plazo no mayor de tres días hábiles después de recibida aquella.

La respuesta a la solicitud es de obligatorio cumplimiento y no deberá estar condicionada (art. 28-33), e caso de ser denegatoria, deberá estar debidamente motivada bajo pena de nulidad, contra la cual cabe recurso de apelación (art. 35 y 37).

Ahora, si la autoridad competente no da respuesta a la solicitud dentro del plazo establecido, se considerará como una aceptación de lo pedido siempre y cuando la información solicitada no tenga carácter de reservada o confidencial (art. 36).

Finalmente, se establecen también sanciones administrativas impuestas a los servidores cuando incurran en alguna de las faltas reguladas por la ley (art. 47-49)

1.1.7. Código Procesal Penal.[97]

El Código procesal penal nicaragüense data del año 2001, y a través de él se procesan y sancionan los delitos consagrados en la Ley 1042, ley especial de ciberdelitos, pues la misma no cuenta con su propio proceso especial, sino que utiliza este código como norma procesal supletoria.

- **Etapa inicial (investigación):**

El proceso penal comienza con la ejecución de los actos iniciales comunes, esto es, la denuncia, las actuaciones policiales y demás investigaciones que requieren de autorización judicial, finalizando con las actuaciones del Ministerio Publico (art. 222-252).

Una vez recibida la denuncia, el Ministerio Publico la estimará (art. 246) o desestimará (art. 226), o también puede suceder que no dé respuesta alguna, para lo cual se procederá de acuerdo a lo estipulado en este Código (art. 225).

En la investigación podrá participar también el Ministerio Público, sin que ello implique la realización de actos que, por su naturaleza, correspondan a la Policía Nacional, la cual podrá también recibir orientaciones por parte del aquel sobre los actos investigativos (art. 248)

Igualmente, el Ministerio Público podrá llevar registro de las actuaciones, citar a cualquier persona que considere pertinente, solicitar información a funcionarios o empelados del Estado, y realizar cualquier otra actividad que considere necesaria para la a búsqueda de elementos de convicción, conforme a la ley (art. 249-252).

Ahora bien, en el caso de los ciberdelitos, en lo que respecta a la conservación de datos, la Ley especial de Ciberdelitos señala que, tanto la Policía Nacional como el Ministerio Publico deberán actuar con la con la celeridad requerida, principalmente cuando exista riesgo de pérdida o modificación (art. 37). Y, relativo a las medidas

97. Nicaragua. Ley No. 406, “Código Procesal Penal de Nicaragua”. *La Gaceta - Diario Oficial*, del 21 y 24 de diciembre del 2001, Nos. 243 y 244. Disponible en: https://www.poderjudicial.gob.ni/pjupload/spenal/pdf/2001_ley02.pdf

de aseguramiento, sin perjuicio de cualquier otra que pueda aplicarse, se podrá solicitar (art.38):

- La incautación y depósito de sistemas informáticos o dispositivos de almacenamiento de datos.
- El sellado, precinto y prohibición de uso de sistemas informáticos o dispositivos de almacenamiento de datos.
- El requerimiento de preservación inmediata de datos que se hallen en poder de terceros.
- La copia de datos.

Igualmente, en la etapa de investigación, ya sea para obtener o conservar información contenida en los sistemas informáticos o cualquiera de sus componentes, se requerirá de autorización judicial por cualquier Juez de Distrito de lo Penal, autorización que deberá ser solicitada por la Policía o por el Ministerio Público. Las actuaciones que para este efecto puede ordenar el Juez, son las ya previstas en la ley (art. 39).

- **Etapa intermedia (audiencia preliminar/audiencia inicial y auto de remisión a juicio).**

Una vez finalizada la etapa investigativa, y practicadas las diligencias por parte de la Policía Nacional y el Ministerio Público para la correspondiente acusación, se procederá a dar inicio a la etapa intermedia, la cual comenzará con la audiencia preliminar si hay reo detenido, sino lo hay, con la audiencia inicial (art. 254, 255-267, 265-272)

Realizadas todas las actuaciones correspondientes y si se considera la procedencia de la acusación, se dictará auto de remisión a juicio, en donde se indicará, entre otras cosas, la fecha, lugar y hora del juicio oral y público (art. 272).

- **Etapa de Juicio (celebración de juicio, deliberación y sentencia):**

El juicio será oral, público, grabado, concentrado y contradictorio, sin embargo, algunas de estos principios, podrán ser condicionados por la autoridad judicial, o

podrá haber excepciones de su aplicación, en los casos y de acuerdo a lo previsto por este Código (art. 283-291).

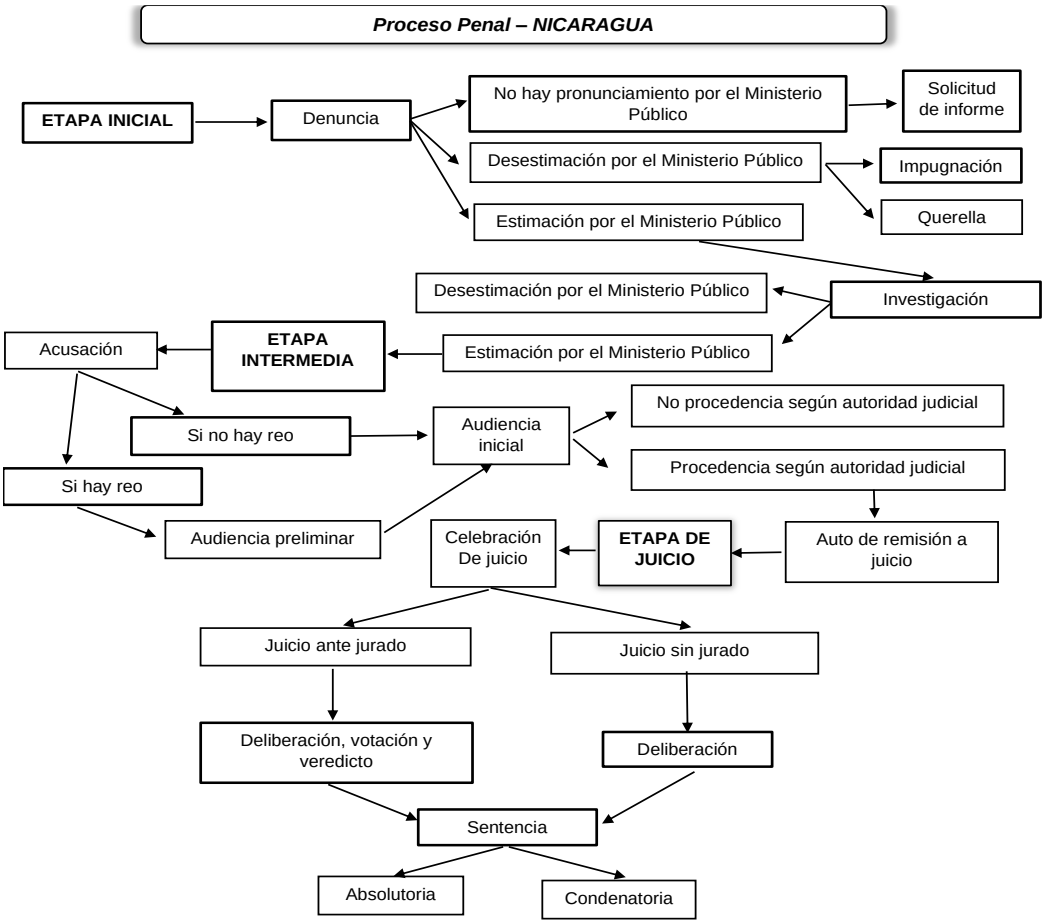
En el juicio, el juez, el Ministerio Publico, el acusador particular si hubiere, los miembros del jurado si fuere el caso, el acusado y su defensor, deben estar presentes de forma ininterrumpida, no suspendiéndose por la ausencia de los sujetos expresamente establecidos.

Ahora bien, el juicio podrá llevarse a cabo ante jurado, pero solo en los casos en donde se acuse por un delito grave, excepto en las causas por delitos relacionados con el consumo o tráfico de estupefacientes, sicotrópicos y otras sustancias controladas o con lavado de dinero y activos provenientes de actividades ilícitas (art. 293-302). En estos casos el juez se encargará únicamente de presidir el juicio, resolver las cuestiones legales e instruir al jurado (art. 298).

En lo que respecta al desarrollo del juicio, una vez que se haya verificado la presencia de las partes, los defensores y los integrantes del jurado cuando corresponda, se procederá a la realización de las actuaciones establecidas en este cuerpo normativo, que van desde la promesa de ley al jurado (cuando corresponda), la lectura de la acusación, exposición de la parte acusada y la parte defensora, práctica de las pruebas, … hasta la exposición de los alegatos finales, pudiendo clausurarse anticipadamente le juicio en los casos que la ley establece. (art. 303-315).

Una vez practicadas todas estas actuaciones, se procederá la deliberación (art. 316-323). La cual podrá resultar en veredicto o fallo de no culpabilidad o de culpabilidad, y en ambos casos el juez se encargará de ordenar lo procedente. La discusión de la pena, podrá realizarse en la misma audiencia o en una convocada; posteriormente se le concederá la palabra a la parte acusadora y a la parte defensora para que debatan sobre la pena o medidas a imponer; seguidamente se le dará la palabra al condenado por si desea hacer alguna manifestación (art. 322). Finalmente, dentro de los tres días posteriores al debate de la pena, se dictará la sentencia que corresponda en una nueva audiencia convocada (art. 323).

Gráfico 3. *Proceso penal nicaragüense*. En este gráfico se muestra el proceso penal ordinario nicaragüense, aplicable también a la materia ciberdelictual.



Fuente: Elaboración propia

1.2. Costa Rica.

1.2.1. Constitución Política.[98]

La constitución política costarricense del año 1949, garantiza el derecho a la intimidad, a la libertad y al secreto de las comunicaciones, ya sean estas escritas

98. Costa Rica. Constitución Política de la República de Costa Rica con reformas incorporadas. *Colección de leyes y decretos*, año 1949, semestre 2, tomo 2, p. 724. Disponible en: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=871&nValor3=0&strTipM=TC

orales o de cualquier tipo, por lo cual se incluyen aquellas practicadas a través de medios cibernéticos.

Fijando la ley en cuáles casos podrán los Tribunales de Justicia ordenar que se intervenga cualquier tipo de comunicación e indicando los delitos en cuya investigación podrá autorizarse el uso de dicha potestad y durante cuánto tiempo (art. 24).

Asimismo, La Sala Constitucional, en la sentencia 5802-99 de las 15:36 h. del 27 de julio de 1999, menciona que la recolección de los datos debe darse con base en el consentimiento del sujeto o con la autorización de la ley.

La normativa relacionada con la protección del derecho de la privacidad es la Ley No. 8968, Ley de Protección de la Persona frente al Tratamiento de sus datos Personales, y la Ley No. 9048, Ley de Reforma de varios artículos y modificación de la Sección VIII, denominada Delitos Informáticos y Conexos, del Título VII del Código Penal.

Por otro lado, la Constitución señala que nadie puede ser inquietado ni perseguido por la manifestación de sus opiniones ni por acto alguno que infrinja la ley (art. 28).

En el mismo sentido, expresa que todos pueden comunicar sus pensamientos de palabra o por escrito, y publicarlos sin previa censura; pero serán responsables de los abusos que cometan en el ejercicio de este derecho, en los casos y del modo que la ley establezca (art. 29).

Indica también la garantía del libre acceso a los departamentos administrativos con propósito de adquirir información sobre asuntos de interés público, quedando a salvo los secretos de Estado (art.30).

1.2.2. Código Penal.[99]

Costa Rica no cuenta actualmente con una ley especial sobre ciberdelincuencia, sino que regula esta materia a través de su Código Penal, el cual data del año 1970, y en el empiezan a normarse los delitos informáticos a partir del año 2001, con la promulgación de la Ley 8148, en la cual se adicionan al Código Penal los artículos de Violación de comunicaciones electrónicas, Fraude Informático y Alteración de datos y Sabotaje informático.

Actualmente la gama de conductas delictivas tipificadas ha aumentado debido a las múltiples reformas que se han realizado, principalmente con el objetivo de adaptar la normativa al Código de Budapest.

Así, la última reforma realizada data del año 2012 con la promulgación de la Ley No. 9048, denominada "Reforma de la SECCIÓN VIII, DELITOS INFORMÁTICOS Y CONEXOS, del TÍTULO VII del Código Penal"[100], a través de la cual se modificaron varios artículos del Código Penal, dándose los cambios principalmente en el aumento de las penas e inclusión de conductas relacionadas con el uso de redes sociales, medios informáticos, entre otros. Asimismo, fueron adicionados algunos incisos e incorporado otros tipos penales no previstos con anterioridad.

Por último, se agregó la "SECCIÓN VIII", es decir, la que fue objeto de reforma, al TÍTULO VII de los "DELITOS CONTRA LA PROPIEDAD", por lo que, actualmente los delitos sancionados en esta materia son:

99. Costa Rica. Ley No. 4573, "Código Penal". *La Gaceta - Diario Oficial*, del 15 de noviembre de 1970, Alcance 120ª, No. 257. Disponible en: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=5027&nValor3=0&strTipM=TC

100. Costa Rica. Ley No. 9048, "Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal". *La Gaceta – Diario Oficial*, del 06 de noviembre de 2012, Alcance 172, No. 214. Disponible en: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=73583&nValor3=90354&strTipM=TC

- **Tipos penales ya regulados con anterioridad y que involucraban el uso de las TICs:**
    - Trata de persona (art. 172).
    - Amenaza a un funcionario público (art. 316).
    - Divulgación de información confidencial (art. 332 *bis*).
    - Injurias (art. 145).
    - Publicación de ofensas (art. 152).
    - Turismo sexual (art. 162 *bis*).
    - Acoso sexual en espacios públicos o de acceso público (art. 388 *bis*)
    - Fabricación, producción, o reproducción de pornografía (art. 173).
    - Tenencia de material pornográfico (art. 173 *bis*).
    - Difusión de pornografía (art. 174).
    - Pornografía virtual y pseudo pornografía. (art. 174 *bis*)
    - Producción de material audiovisual (art. 175).
- **Tipos penales ya regulados, pero reformados para la incorporación de su comisión a través de las TICs o el uso de los medios informáticos:**
    - Corrupción de menores (art. 167).
    - Violación de correspondencia o comunicaciones (art. 196. b).
    - Violación de datos personales (art. 196 bis).
    - Extorsión (art. 214).
    - Estafa informática (art. 217 bis.).
    - Daño informático (art. 229 bis.)
- **Tipo penal ya regulado, pero al cual fue adicionado el inciso 6):**
    - Daño agravado (art. 229. 6).
- **Tipo penal no previsto con anterioridad:**
    - Sabotaje informático (art. 229 ter.).
- **Tipos penales ya regulados con anterioridad, pero modificados:**
    - Suplantación de identidad (art. 230).
    - Espionaje informático (art. 231).
    - Instalación o propagación de programas informáticos maliciosos (art. 232).

- Suplantación de páginas electrónicas (art. 233)
- Facilitación de los medios para la consecución del delito informático (art. 234).
- Narcotráfico y crimen organizado (art. 235).
- Difusión de información falsa (art. 236).

1.2.3. Ley N. ° 8968, de Protección de la Persona frente al Tratamiento de sus Datos Personales.[101]

La Ley No. 8968 Protección de la Persona frente al Tratamiento de sus Datos Personales y su Reglamento, data del año 2011, y nace con el objetivo de asegurar la privacidad de los datos personales referentes a la persona misma o sus bienes.

No considerando aquellos datos mantenidos por personas físicas o jurídicas con fines exclusivamente internos, personales o domésticos, mientras no sean comercializados (art. 2). En todo caso, aquellas bases de datos pública o privada, administrada con fines de distribución, difusión o comercialización, debe inscribirse en el registro que al efecto habilite la Prodhab, del que se hablará más adelante (art. 21).

Esta ley tiene como principio fundamental el derecho a la autodeterminación informática (art. 4), el cual implica el legítimo tratamiento de los datos personales bajo la previsión del derecho a la privacidad, y la prohibición de discriminación respecto de los mismos. Habiendo excepciones a la aplicación de este principio (art.8), por ejemplo, por razones de seguridad de Estado.

Sobre esto, la ley categoriza los datos en cuatro tipos (art. 9):

- **Datos sensibles:** Los cuales ninguna persona está obligada a suministrar, salvo los casos expresos por la ley.

101. Costa Rica. Ley No. 8968, "Ley de Protección de la Persona frente al tratamiento de sus datos personales". *La Gaceta – Diario Oficial,* del 05 de septiembre de 2011, Nº. 170. Disponible en: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=70975&nValor3=85989&strTipM=TC

- **Datos personales de acceso restringidos:** Solo serán utilizados para fines públicos o con consentimiento expreso.
- **Datos personales de acceso irrestricto:** Son los contenidos en bases de datos públicas de acceso general.
- **Datos referentes al comportamiento crediticio:** Se regirán por las normas que regulan el Sistema Financiero Nacional.

Asimismo, se establecen responsabilidades a los sujetos encargados de la recolección, el almacenamiento y el uso de datos personales, los cuales podrán emitir un protocolo de actuación en el cual establecerán los pasos que deberán seguir para estas actuaciones de conformidad con las reglas previstas en esta ley, los cuales solo tendrán valor una vez inscritos (art.12).

En caso de que una base de datos pública o privada actúe en contravención de las reglas o los principios básicos deberá agotarse primeramente la vía administrativa siguiendo el proceso y cumplimiento con los requisitos formales establecidos en la presente ley (art. 23-26); en cuyo caso se impondrán las sanciones que correspondan si resulta procedente (art. 28-32).

Asimismo, a través de esta ley se crea la Agencia de Protección de Datos de los Habitantes (Prodhab) (art. 15-20), una institución de desconcentración máxima adscrita al Ministerio de Justicia y Paz, con independencia de criterio y personalidad jurídica instrumental propio en el desempeño de las funciones y en la administración de sus recursos y presupuesto, así como para suscribir los contratos y convenios que requiera para el cumplimiento de sus funciones.

1.2.4. Código Procesal Penal.[102]

A través del Código Procesal de Costa Rica del año 1996, se procesan y sancionan los delitos cibernéticos consagrados en el TÍTULO VII, SECCIÓN VIII del Código Penal.

102. Costa Rica. Ley No. 7594, “Código Procesal Penal”. *La Gaceta – Diario Oficial*, del 04 de junio de 1996, Alcance 31, No. 106. Disponible en:

Cabe mencionar que, podrá aplicarse también en el caso de los ciberdelitos, algún procedimiento especial cuando el asunto así lo requiera, ya sea a razón de conformidad de las partes o aceptación del hecho por el imputado (Procedimiento abreviado, art. 373-375); la complejidad del asunto (Procedimiento para asuntos de tramitación compleja, art. 376-379); debido al tipo de acción penal (Procedimiento por delito de acción privada, art. 380-387); o debido a otras circunstancias previstas en este Código.

- **Etapa pre-procesal (investigación):**

El proceso penal comienza por la etapa de investigación (art. 278-297), la cual se genera con la denuncia, querella, u otro requisito equivalente y concluye cuando el imputado queda a disposición del juez

Esta investigación puede llevarse a cabo por parte de funcionarios o agentes de la policía judicial o bien por el Ministerio Publico, cuando corresponda.

- **Etapa intermedia (acusación, audiencia preliminar y auto de apertura a juicio):**

Una vez finalizada la etapa investigativa, tiene lugar la etapa intermedia o preparación de juicio (art. 303-322, 324-340), la cual comienza con la formulación de la acusación y concluye con el auto de apertura a juicio y tiene por objeto el ofrecimiento y admisión de los medios de prueba, así como la depuración de los hechos controvertidos que serán materia de juicio.

Esta etapa se compone de dos fases:

  - **Fase escrita:** Se refiere al escrito de acusación que formula el Ministerio Publico una vez que estima que la investigación proporciona fundamento para someter a juicio público al imputado.

http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=41297&nValor3=0&strTipM=TC

- **Fase oral:** Se refiere a la celebración de la audiencia intermedia en donde el tribunal resolverá inmediatamente y de forma oral las cuestiones planteadas, salvo casos excepcionales.

Si se resuelve la procedencia de la acusación, se realizará el auto de apertura a juicio, el cual dará por terminada la presente etapa, y en la que se indicará la parte de la acusación o de la querella que resulte admitida; la disposición de enviar a juicio el asunto; y el emplazamiento a las partes.

Durante las cuarenta y ocho horas siguientes de recibidas las diligencias, se fijarán el día y la hora del juicio, el cual podrá celebrarse en dos fases.

- **Etapa de juicio (celebración de juicio y emisión de sentencia):**

La etapa de juicio oral y público (art. 341-396) comienza con su sustanciación y finaliza con la emisión de la sentencia correspondiente.

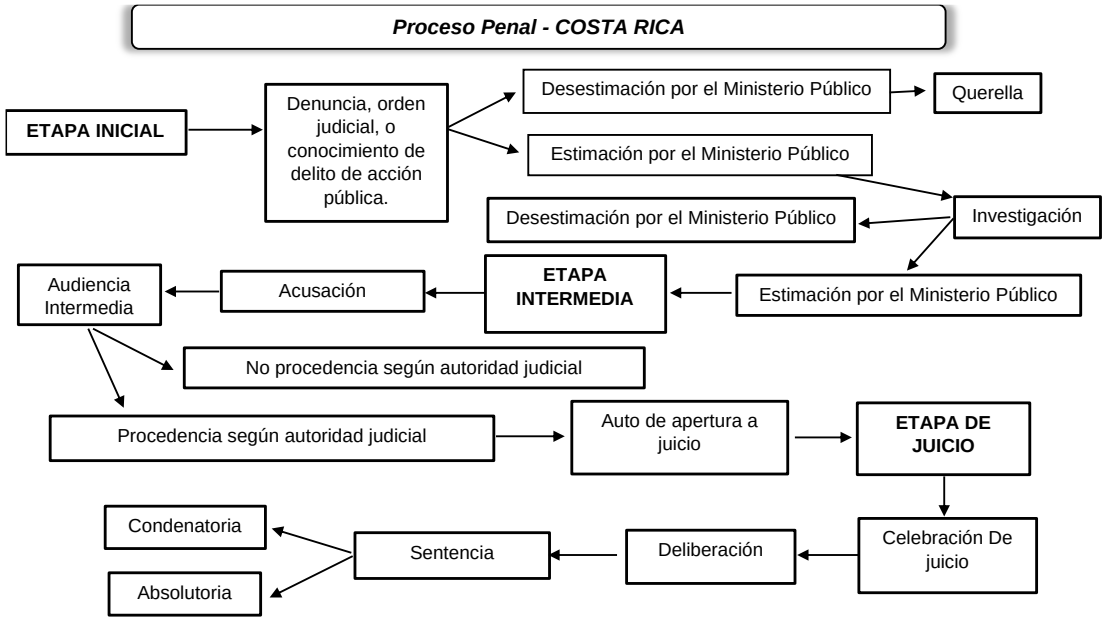
Así, durante el juicio y una vez verificada la presencia de las partes, los testigos, peritos e intérpretes se dará apertura al juicio procediéndose de la manera establecida en el Código, comenzando desde la lectura de la acusación, la resolución de los incidentes, recibimiento de pruebas, interrogatorio, …hasta la discusión final.

Realizadas las diligencias, se procede a la deliberación y sentencia, proceso que no podrá extenderse más allá de dos días, salvo casos complejos o causas justificadas, en caso contrario, el juicio se deberá repetir ante otro tribunal.

El juicio podrá reabrirse, durante la deliberación y solo en caso de que el tribunal lo consideren estrictamente necesario, ya sea para recibir nuevas pruebas, o ampliar las ya incorporadas.

La sentencia podrá ser condenatoria o absolutoria y dará lugar a las actuaciones que correspondan según la ley.

Gráfico 4. *Proceso penal costarricense.* En este gráfico se muestra el proceso penal ordinario costarricense, aplicable también a la materia ciberdelictual.



Fuente: Elaboración propia

1.3. El Salvador.

1.3.1. Constitución Política.[103]

La constitución política salvadoreña parte del reconocimiento de la persona humana como objeto y fin de la actividad estatal, para la consecución de la justicia, la seguridad jurídica y el bien común; por lo que asegura reconocer como obligación del Estado, para con sus habitantes, el goce de la libertad, la salud, la cultura, el bienestar económico y la justicia social.

Reconociendo como parte de los derechos individuales, en sus arts. 2 y 3, el derecho a la integridad física y moral, a la libertad, a la seguridad, a la propiedad…

103. El Salvador. Decreto No. 38, "Constitución Política de la Republica de El Salvador". Actualizada hasta las reformas del Decreto No. 707. *La Gaceta – Diario Oficial*, del 19 de junio de 2014, Tomo No. 403, No. 112. Disponible en:https://www.asamblea.gob.sv/sites/default/files/documents/decretos/171117_072857074_archivo_documento_legislativo.pdf

afirmando la protección del individuo en la conservación y defensa de los mismos. Garantizando además el derecho al honor, a la intimidad personal y familiar y a la propia imagen, considerando propicio de indemnización los daños de carácter moral, dado que reconoce los derechos civiles de forma igualitaria, rechazando toda restricción o privilegio en base a desigualdades.

Expresando, en su art. 6, muy detalladamente el reconocimiento a la libre expresión y difusión de pensamientos, siempre que esto no contravenga el orden público, la moral, el honor, ni la vida privada de las personas; no obstante, advierte que, aunque el ejercicio de dicho derecho no está sujeto a previo examen, ni censura, ni caución, podrá ser objeto de ilicitud, cuando este infrinja la ley, por lo que no se exenta de responsabilidad penal. Y además reconoce el derecho de respuesta como protección de los derechos y garantías fundamentales.

Y con respecto al derecho de inviolabilidad de domicilio, correspondencia y comunicaciones, sus artos 20 y 24, establecen su resguardo y fortalecimiento al detallar los casos en que se restringe y establecer que su violación da derecho a indemnización por los daños y perjuicios ocasionados.

1.3.2. Código Penal.[104]

El código penal salvadoreño vigente incluye algunos delitos que contemplan las TICs como medio para la realización de la conducta típica antijurídica, pero no regula los delitos informáticos propiamente dicho; es decir, se tratan de conductas criminógenas que se valen de las TICs como método, medio o símbolo en la comisión del ilícito.

104. El Salvador. Decreto No. 1030, “Código Penal”. Actualizado hasta las reformas del Decreto No. 374. *La Gaceta – Diario Oficial*, del 14 de junio de 2022, Tomo No. 435, No. 112. Disponible en: https://www.jurisprudencia.gob.sv/busqueda/showFile.php?bd=2&data=DocumentosBoveda%2FD%2F2%2F1990-1999%2F1997%2F06%2F886E3.PDF&number=558819&fecha=10/06/1997&numero=CODIGO=PENAL&cesta=0&singlePage=false%27

Encontrándose vinculados a los delitos propiamente informáticos, entre los delitos contra la libertad sexual, la pornografía infantil (art 173); entre los delitos relativos al honor y la intimidad, la calumnia (art. 177), difamación (art. 178) e injuria (art.179); entre los delitos relativos a la intimidad, la violación de comunicaciones privadas (art. 184), violación agravada de comunicaciones (art. 185) y captación de comunicaciones (art.186); entre los delitos relativos al patrimonio, los daños agravados (art. 222.2).

1.3.3. Decreto No. 260, Ley especial contra los delitos informáticos y conexos.[105]

Tras la fuerza trascendental que han adquirido los instrumentos electrónicos empleados para el envío, resguardo y recepción de información, tanto a nivel internacional como nacional, para el desarrollo económico, político, social y cultural, el Estado Salvadoreño, tras considerar insuficientes sus instrumentos normativos vigentes, decide promulgar la LEDIC, para priorizar la protección de la confidencialidad, integridad, seguridad y disponibilidad de la información, y así mismo facilitar la detección, investigación y sanción de tan diversas actividades delictivas.

Estableciendo como su objeto la protección tanto de los bienes jurídicos que se pueden ver amenazados por el mal empleo de las TICs, como la prevención y sanción de los delitos cometidos en perjuicio de los datos almacenados, procesados o transferidos; los sistemas, su infraestructura o cualquiera de sus componentes, o los contenidos mediante el uso de dichas tecnologías que afecten intereses asociados a la identidad, propiedad, intimidad e imagen.

Siendo, para su salvaguarda, muy detallados respecto al ámbito espacial de la norma, al indicar que esta se aplicara:

105. El Salvador. Decreto No. 260, “Ley especial contra los delitos informáticos y conexos”. Actualizada hasta las reformas del Decreto No. 236. *La Gaceta – Diario Oficial*, del 12 de enero de 2022, Tomo No. 434, No. 8. Disponible en:https://www.jurisprudencia.gob.sv/DocumentosBoveda/D/2/2010-2019/2016/02/B6B74.PDF

- A los hechos punibles cometidos total o parcialmente en el territorio nacional o en lugares sometidos a su jurisdicción.
- A cualquier persona, natural o jurídica, nacional o extranjera, por delitos que afecten bienes jurídicos del Estado, sus habitantes o protegidos por pactos o tratados internacionales ratificados por El Salvador.
- Si la ejecución del hecho se inició en territorio extranjero y se consumó en el territorio nacional o si se hubiesen realizado, utilizando TICs instaladas en el territorio nacional y el responsable no haya sido juzgado por el mismo hecho en tribunales extranjeros o haya evadido el juzgamiento o condena.

Y encontrándonos a lo largo de este cuerpo normativo la tipificación y adopción de medidas, así como el señalamiento de penas, aplicables a los ciberdelitos en el contemplados, consistiendo estos, según su orden y características del delito, en: delitos contra los sistemas tecnológicos de información (art. 4-9), delitos informáticos (art. 10-14), delitos informáticos relacionados con el contenido de los datos (art. 15-27), delitos informáticos contra niñas, niños y adolescentes o personas con discapacidad (art. 28-33), delitos contra el orden económico (art. 34).

Siendo todas sus sanciones aplicables sin perjuicio de otras responsabilidades penales, civiles o administrativas.

1.3.4. Decreto No. 551, Ley especial para sancionar infracciones aduaneras, énfasis en delitos informáticos.[106]

El Decreto No. 551, Ley LESIA, fue promulgado mediante decreto legislativo el 20 de septiembre de 2001 y publicado en el Diario Oficial No. 204, tomo No. 353 del 29 de octubre de 2001. Y dicho cuerpo normativo, desde su origen y hasta la fecha, contempla un tipo penal que designo como “delitos informáticos”.

106. El Salvador. Decreto No. 551, “Ley especial para sancionar infracciones aduaneras”. Actualizada hasta las reformas del Decreto No. 18. *La Gaceta – Diario Oficial*, del 05 de junio de 2018, Tomo No. 419, No. 102. Disponible en:https://www.jurisprudencia.gob.sv/DocumentosBoveda%2FD%2F2%2F2000-2009%2F2001%2F10%2F889FF.PDF

Contenido en su art. 24, bajo la denominación de delitos informáticos, este sanciona con pena de prisión de tres a cinco años a quien:

- Acceda, sin la autorización correspondiente y por cualquier medio, a los sistemas informáticos utilizados por la Dirección General;
- Se apodere, copie, destruya, inutilice, altere, facilite, transfiera o tenga en su poder, sin autorización de la autoridad aduanera, cualquier programa de computación diseñado por o para tal autoridad o sus bases de datos, que de manera exclusiva y en ejercicio de sus controles y servicios utilizare la Dirección General;
- Dañe los componentes materiales o físicos de los aparatos, las maquinas o accesorios que apoyen el funcionamiento de los sistemas informáticos o de comunicaciones, diseñados para las operaciones de la Dirección General, con la finalidad de entorpecerlas u obtener beneficio para sí o para otra persona;
- Facilite el uso del código y clave de acceso, asignados para ingresar en los sistemas informáticos.
- Manipule el sistema informático o de comunicación a fin de imposibilitar cualquier control que con base en dicho sistema exista la posibilidad de realizar.

De donde podemos observar que, todas las conductas antes mencionadas, a excepción de la tercera, recogen un tipo penal o más de uno, de los ya comprendidos en la LEDIC, como lo vemos en el:

- Primer supuesto: Acceso indebido a sistemas informáticos; acceso indebido a programas o datos informáticos; y violación de la seguridad del sistema (artos. 4, 5 y 9);
- Segundo supuesto: Daños a sistemas informáticos; posesión de equipos o prestación de servicios para la vulneración de la seguridad; y alteración, daño a la integridad y disponibilidad de los datos (artos. 7, 8 y 19);
- Cuarto supuesto: Divulgación no autorizada (art. 23); y
- Quinto supuesto: Manipulación de registros (art. 15).

1.3.5. Decreto No. 108, Ley contra actos de terrorismo, énfasis en delitos informáticos.[107]

El Decreto No. 108, Ley LCAT, fue promulgado mediante decreto legislativo el 11 de octubre de 2006 y publicado en el Diario Oficial No. 193, tomo No. 373 del 17 de octubre de 2006. Y dicho cuerpo normativo, desde su origen y hasta la fecha, contempla un tipo penal que designo como “delitos informáticos”.

Contenido en su art. 12, bajo la denominación de delito informático, este sanciona con pena de prisión de diez a quince años a quien:

- Utilizare equipos, medios, programas, redes informáticas o cualquier otra aplicación informática para interceptar, interferir, desviar, alterar, dañar, inutilizar o destruir datos, información, documentos electrónicos, soportes informáticos, programas o sistemas de información y de comunicaciones o telefónicos, de servicios públicos, sociales, administrativos, de emergencia de seguridad nacional, de entidades nacionales, internacionales o de otro país;
- Creare, distribuyere, comerciare o tuviere en su poder programas capaces de producirlos efectos a que refiere el literal a), de este artículo.

De donde podemos observar que todas las conductas antes mencionadas recogen un tipo penal o más de uno, de los ya comprendidos en la LEDIC, como lo vemos en el:

- Primer supuesto: Acceso indebido a sistemas informáticos; acceso indebido a programas o datos informáticos; Daños a sistemas informáticos; violación de la seguridad del sistema; y alteración, daño a la integridad y disponibilidad de los datos (artos. 4, 5, 7, 9 y 19); y

107. El Salvador. Decreto No. 108, “Ley especial contra actos de terrorismo”. Actualizada hasta las reformas del Decreto No. 341. *La Gaceta – Diario Oficial*, del 30 de marzo de 2022, Tomo No. 434, No. 65. Disponible en:https://www.jurisprudencia.gob.sv/busqueda/showFile.php?bd=2&data=DocumentosBoveda%2FD%2F2%2F2000-2009%2F2006%2F10%2F889E6.PDF&number=559590&fecha=17/10/2006&numero=LEY=ESPECIAL=CONTRA=ACTOS=DE=TERRORISMO&cesta=0&singlePage=false%27

- Segundo supuesto: posesión de equipos o prestación de servicios para la vulneración de la seguridad (art. 8).

1.3.6. Código Procesal Penal.[108]

El decreto legislativo No. 733, Código Procesal Penal Salvadoreño, del 22 de octubre de 2008, inicialmente publicado en el diario oficial No. 20, tomo 382, del 30 de enero de 2009, con sus reformas incorporadas, mediante decreto legislativo No. 339; establece el procedimiento común a las etapas del proceso penal Salvadoreño, cuyos parámetros extienden su aplicación al proceso y sanción de los delitos cibernéticos contemplados en LEDIC, considerando algunas características propias, para los actos de investigación y de pruebas, así como la cadena de custodia, en delitos que impliquen el empleo de las TICs (artos. 201 y 259 A-E).

No obstante, podrá aplicarse en el caso de los ciberdelitos, algún procedimiento especial cuando el asunto así lo requiera, ya sea a razón de conformidad de las partes o aceptación del hecho por el imputado (procedimiento abreviado artos. 417-418CPP); debido al tipo de acción penal (procedimiento por delito de acción privada artos 439-444CPP); o debido a otras circunstancias previstas en este código.

- **Etapa inicial (Actos iniciales comunes: Denuncia; Querella; diligencias de investigación; y requerimiento):**

El proceso penal parte de la puesta en conocimiento, a las autoridades competentes, de la comisión de un posible hecho ilícito (*notitia criminis*), mediante la denuncia o la querella (107, 109, 110, 118, 261 y 263) en los casos que corresponda y bajo las excepciones previstas, considerando que la denuncia y la

108. El Salvador. Decreto No. 733, "Código Procesal Penal". Actualizado hasta las reformas del Decreto No. 339. *La Gaceta – Diario Oficial*, del 30 de marzo de 2022, Tomo No. 434, No. 65. Disponible en: https://www.jurisprudencia.gob.sv/busqueda/showFile.php?bd=2&data=DocumentosBoveda%2FD%2F2%2F2000-2009%2F2009%2F01%2F89AA7.PDF&number=563879&fecha=30/01/2009&numero=CODIGO=PROCESAL=PENAL&cesta=0&singlePage=false%27

querella contienen calidades necesarias diferentes, de forma y contenido, al momento de su interposición (108, 162, 267, 268 y 269).

Así pues, presentada la denuncia o querella se procede a la confirmación de la "notitia criminis" y, en su caso, a proporcionar al Ministerio Público los elementos necesarios para promover la acción penal, que se ejercita a través del correspondiente requerimiento fiscal, dando así lugar al inicio del proceso penal propiamente dicho. [109]

Realizándose para esto las diligencias correspondientes (art. 270, 271y 272) por parte de la fiscalía general y la policía, así como los actos coordinados, para la investigación de los hechos punibles.

La investigación estará en cualquier caso bajo el control fiscal, sin perjuicio de la autoridad general administrativa a la que los oficiales y agentes policiales se encuentren sometidos; siendo el fiscal el encargado de dirigir la investigación, pudiendo disponer en cualquier momento de las actuaciones policiales o estableciendo un plazo para su conclusión.

En lo referente a la forma de las diligencias previas de investigación, es obligación de la autoridad policial documentar las constancias y diligencias de toda la actividad investigativa, con la mayor exactitud posible, en actas y diligencias que deberán firmar quien ha dirigido la investigación y todas las personas, funcionarios o particulares, que hayan intervenido en cada una de las diligencias, incluido el defensor del imputado si hubiere concurrido a la misma.

Asimismo, se incorporará a la investigación preliminar, dos tipos de diligencias, las objetivas y subjetivas; refiriéndose las objetivas o de hecho a los hechos averiguados y a las circunstancias que se hubieren observado y pudiesen ser prueba o indicio de delito, documentado mediante diligencias de constatación. Y las subjetivas, generalmente, a declaraciones personales de los imputados o testigos,

109. CASADO, José. Et al. Op. Cit. pp. 886-890

incluidas las de los propios agentes respecto de los hechos conocidos personalmente. [110]

A estas diligencias se añaden las medidas cautelares o de aseguramiento, tanto reales, recogida del cuerpo y efectos del delito, como personales, aprehensión de los imputados.

Finalizadas las diligencias investigativas, tiene lugar el requerimiento fiscal, acto procesal que realiza el ministerio público a fin de promover el comienzo de la actividad instructora, proporcionando elementos de juicio suficientes respecto del delito presuntamente cometido y de la identificación del autor.[111]

El requerimiento fiscal se promueve una vez concluidas las diligencias iniciales de investigación y dentro de los plazos establecidos, disponiendo el fiscal, conforme lo establecido en el art. 294-ACPP, de 72 horas para formular su requerimiento ante el juez de paz, si el sospechoso se encuentra detenido, en caso contrario, contara con 10 días para su presentación, una vez concluidas las investigaciones, y 20 días en los casos de crimen organizado y delitos de realización compleja.

Pudiendo solicitar, de ser necesario, que se decrete o mantenga la detención provisional u otra medida cautelar al imputado. Y si faltare alguno de los requisitos antes mencionados, el juez podrá ordenar, en un plazo de tres días, de no haber detenido, o lo hará durante la audiencia inicial de haberlo, su indicación, y de no ser completados dichos datos se declarará inadmisible.

Cabe destacar que entre las diversas solicitudes que puede formular el fiscal mediante el requerimiento, no solo se contempla la petición de instrucción formal, sino que atendiendo al resultado de la investigación inicial, el requerimiento fiscal puede tener diversas finalidades, conforme el art. 295CPP, y solicitar: la desestimación de la denuncia, el sobreseimiento, la aplicación de criterios de

110. CASADO, José. Et al. Op. Cit. pp. 914-918

111. CASADO, José. Et al. Op. Cit. pp. 923-932

oportunidad, la suspensión del procedimiento de prueba, la incoación del procedimiento abreviado, e incluso, la conciliación o mediación.

Cuya resolución será debidamente notificada a las partes, y en caso de inconformidad de alguna de ellas, el fiscal presentará el requerimiento respectivo solicitando al juez competente la desestimación o el sobreseimiento en su caso.

- **Etapa Intermedia: (Audiencia inicial; Audiencia preliminar / Etapa de instrucción)**

    - **Audiencia inicial:**

La presente etapa comienza con la audiencia inicial, que, como su nombre lo indica, supone la primera intervención judicial de importancia en la resolución del caso, a través de la cual se concreta el alcance de la imputación, permite al fiscal individualizar los cargos y delimitar el alcance de la investigación que habrá de desarrollarse en la instrucción. Siendo posible también decidir en esta audiencia, la incoación del proceso o, en su caso, sobre algunas de las pretensiones alternativas formuladas por el ministerio fiscal.[112]

Correspondiendo, como lo indica el art. 297CPP, su presupuesto esencial e imprescindible, al requerimiento fiscal, sin el cual no podrá celebrarse su audiencia. Por ello, una vez recibido el requerimiento fiscal, el Juez de Paz convocará a las partes a la celebración de la audiencia, contemplando para la determinación de su plazo la condición del imputado, estipulando, 72 horas de estar detenido o 5 días si no, para su celebración.

Cabe destacar, que la condición del imputado, su detención o no, también afecta al procedimiento a seguir para la realización de esta audiencia, tal como se señala en el art. 298CPP.

112. CASADO, José. Et al. Código Procesal Penal de El Salvador Comentado - Tomo I [En línea]. San Salvador: Consejo Nacional de Judicatura, 2004, pp. 947 y 948. [Consultado el 10 de julio de 2022]. Disponible en: https://www.cnj.gob.sv/images/documentos/pdf/ecj/publicaciones/codigoprocesalpenal_tomoii.pdf

En el desarrollo de la audiencia se verificará el contenido del requerimiento, ordenándose la subsanación cuando sea correspondiente (art. 294); se verificará la presencia de las partes necesarias para la realización de la audiencia; se oirá la declaración del imputado (si está dispuesto); se realizará el interrogatorio (art. 91-92); se escucharán los alegatos de las partes; se podrá solicitar de forma excepcional la incorporación de nuevos medios de prueba; se podrá ampliar el contenido del requerimiento; y, antes de concluir la audiencia el imputado tiene derecho a la última palabra, manifestando a su propia iniciativa lo que tenga por conveniente.

Realizadas estas actuaciones se levantará un acta de la audiencia en la que solamente consten las resoluciones que el juez tome, en relación a los puntos planteados, cuidando evitar la transcripción total de lo ocurrido, de modo que se desnaturalice su calidad de audiencia oral; siendo dicha acta leída al finalizar la audiencia y firmada por las partes, quedando notificación de su lectura.

Luego de escuchar a las partes y, en su caso, de recibir la declaración indagatoria, el juez resolverá las cuestiones planteadas, ordenando las actuaciones que correspondan (art. 300).

Estimándose, en caso de disconformidad, que el Juez remitirá el procedimiento por resolución fundada al fiscal superior, quien dictamina sobre el requerimiento fiscal dentro de los tres días siguientes a la notificación, pudiendo ratificar lo realizado por el fiscal inferior o formular un nuevo requerimiento, a fin de que la autoridad judicial resuelva.

- **Instrucción:**

Ahora bien, si la resolución judicial de control de las diligencias iniciales de investigación estipula que hay mérito para continuar con la indagación del caso, se sigue con la etapa de instrucción formal.

Esta etapa representa una segunda oportunidad para que, después de la fase de audiencia inicial y con mayor disponibilidad de alternativas procesales y de tiempo,

el defensor procure la libertad del imputado y la finalización anticipada del proceso en su contra (artos. 320-342).

En tal sentido, la instrucción es la actividad realizada bajo la coordinación del juez competente (el Juez de Instrucción), para obtener información que permita decidir si procede o no, efectuar un juicio penal y para asegurar su eficacia, en caso que se decida realizarlo. Procurando la mayor colaboración posible entre la fiscalía general de la República, la policía, las partes y las autoridades judiciales.[113]

Por lo que, en cuanto proceda la instrucción, el juez dentro de los tres días siguientes de recibidas las actuaciones, dictará auto sobre el plazo de la misma, actos que requieran autorización judicial, anticipos de prueba y actos necesarios (art. 302).

Recayendo en la autoridad judicial la obligación del cumplimiento de la instrucción antes de la fecha fijada para la audiencia preliminar (art. 309 y 310). Correspondiéndole además realizar los anticipos de prueba, autorizar los actos urgentes de comprobación sujetos a control judicial, resolver sobre las excepciones y demás solicitudes, y controlar el cumplimiento de los derechos y garantías establecidos en la Constitución y las leyes.

Constando todas las diligencias practicadas en sus debidas actas, para la formación de un expediente, en el que se incluirán solo aquellas actas imprescindibles, evitando la acumulación de citaciones, notificaciones o escritos insustanciales.

- **Audiencia preliminar:**

La finalidad de la Audiencia Preliminar es decidir acerca de la procedencia o no de la apertura del juicio oral. Sirviendo de filtro para evitar acusaciones infundadas, sometiéndolas a un debate en presencia del Juez de Instrucción y de las partes, practicándose las diligencias necesarias para la verificación de los elementos de imputación y, en su caso, evitar el juicio oral, cuando no existan elementos

113. CASADO, José. Et al. Op. Cit. pp. 1008-1012

incriminatorios suficientes en contra del imputado o si existe la posibilidad de optar por un medio alternativo de finalización del proceso.[114]

Pudiendo el fiscal y el querellante proponer hasta 5 días después de concluida la instrucción para presentar la acusación; solicitar sobreseimiento, criterio de oportunidad, procedimiento abreviado, o bien homologación de los acuerdos (art. 355). Apreciándose, asimismo, el establecimiento de una serie de presupuestos que habrán de cumplirse bajo pena de inadmisibilidad (art. 356).

Para así, una vez presentada la acusación o demás solicitudes previstas, el Juez de Instrucción, en un plazo de 24 horas, ponga a disposición de todos las partes las actuaciones y las evidencias, para que puedan consultarlas en el plazo común de 5 días; los que, finalizados, facultarán al juez para el señalamiento de la audiencia preliminar en un plazo no menor de 3 días ni mayor de 15 días.

Concediéndole, en tal caso, a las partes, la disposición de las actuaciones y evidencias recibidas del Ministerio fiscal, a fin de que puedan consultarlas en el plazo de 5 días; aplicables también a favor de las partes para la contestación del dictamen del Ministerio fiscal o del querellante, del que se dará traslado para que, en su caso, puedan impugnar o adherirse al mismo. Para así, una vez recibidas y examinadas las actuaciones poder proponer, solicitar, rectificar, ofrecer, objetar o resolver lo que se tenga a lugar.

Centrándonos ahora específicamente en el ofrecimiento de la prueba, podremos señalar de forma general, que esta habrá de realizarse en tiempo y forma, justificando su pertinencia, necesidad y circunstancias, conforme lo establece este cuerpo normativo (art. 359).

Hecho esto, el juez admitirá o rechazará la prueba ofrecida para la audiencia preliminar, por lo que el juez de instrucción deberá examinar las solicitudes formuladas y aceptar aquellos relevantes para la audiencia, pudiendo ordenar, de

114. CASADO, José. Et al. Op. Cit. pp. 1198-1200

oficio, la práctica de pruebas que considere precisas para la realización de la audiencia.

La Audiencia Preliminar, requiere de la presencia de todas las partes, no obstante, la intervención del querellante no resulta imprescindible y, en caso de que no comparezca, sin causa justificada, se entenderá por abandonada la querella (art. 361); por lo que, a diferencia de la audiencia inicial, en esta audiencia, la presencia del imputado resulta imprescindible, por lo que su falta produce la no realización de la audiencia; debiendo el juez señalar un nuevo día y hora para la realización de la audiencia. No obstante, si la incomparecencia por segunda vez se debe a la negativa del procesado detenido a concurrir, constatado ello por informe del director del presidio respectivo, a juicio prudencial del juez, podrá realizarse la audiencia sin la presencia del mismo.

Dando comienzo la audiencia con la práctica de las diligencias que han sido propuestas por las partes y han sido admitidas por el juez, en donde el juez, además, intentará la conciliación de todas las partes, proponiendo la reparación integral del daño social o particular causado.

Inmediatamente después de finalizar la audiencia, el juez resolverá todas las cuestiones planteadas durante la misma.

- **Etapa Final o Etapa de Juicio: (Juicio Plenario / Vista Pública; Deliberación y Sentencia)**

La etapa final del proceso penal se focaliza en el Juicio Plenario o Vista Pública, proceso encomendado a los Tribunales de Sentencia, donde finalmente se desvirtúa o ratifica la presunción de inocencia.

Imponiendo al presidente del tribunal de sentencia la realización del auto de apertura, quien dentro de las cuarenta y ocho horas de recibidas las actuaciones, fijará el día y la hora de la vista pública, la que no se realizará antes de diez días ni después de un mes.

Celebrándose el juicio en consideración a los principios de inmediación, publicidad y oralidad, conforme lo establecido (art. 367, 369 y 371).

Enmarcando el inicio de las sesiones del juicio oral, en las disposiciones establecidas (art. 367), donde apreciamos la imprescindibilidad de la presencia de las partes. A excepción del querellante, cuya ausencia se asumirá en abandono de la querella, sin perjuicio de que pueda ser obligado a comparecer como testigo.

Constituyéndose el Tribunal en la sala para la celebración de la vista pública, donde seguidamente su presidente procederá a la comprobación de la presencia de las partes, cuya ausencia derivará en consecuencias diversas.

Y así, una vez efectuada la comprobación de las partes, el presidente del Tribunal declarara abierta la vista pública y explicará al imputado la importancia y el significado de lo que va a suceder, indicando que esté atento a lo que va a oír; garantizando que este conozca el sentido de la vista pública, en la que va a ser interrogado y a lo largo de la cual va a oír como quienes en ella intervienen se refieren a él en más de una ocasión, aprovechando a realizarle un somera explicación del desarrollo del juicio, de forma que se garantice, en un sentido amplio, el reconocimiento y promoción de los derechos (art. 82).

Prosiguiendo el comienzo de la parte formal del juicio, mediante la lectura del auto de apertura del juicio oral (art. 380) en el que se describe el hecho justiciable y se designan las personas acusadas, abordando las partes objetivas y subjetivas del objeto de enjuiciamiento; produciéndose a este punto los primeros alegatos de las partes y la tramitación de incidentes.

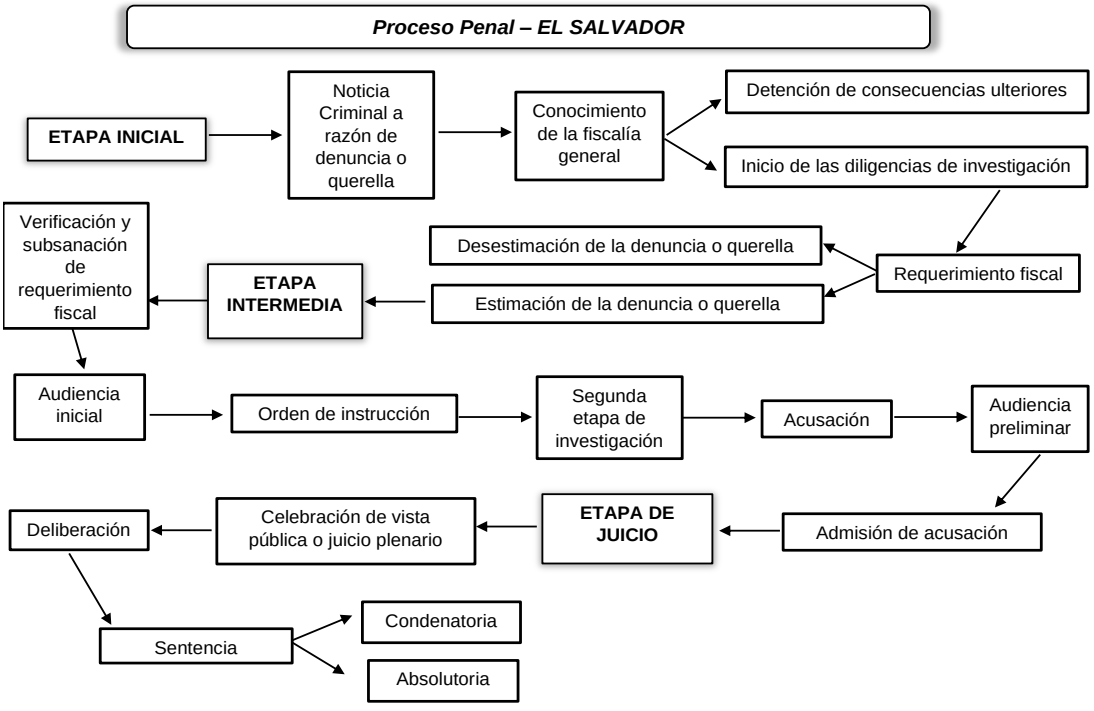
Admitiendo, durante la vista pública, la ampliación de la acusación por parte del fiscal o el querellante, conforme los parámetros establecidos (art. 384), tomándose con posterioridad declaración a la del imputado o los imputados, según las consideraciones definidas (art. 381, 382 y 383) Y el juez recibirá la prueba (art. 386), y otros documentos y elementos audiovisuales (art. 389).

Y, una vez recibida la prueba, se pasa a la discusión final o cierre del debate, concediendo (art. 391), a los intervinientes la facultad de exponer sus conclusiones; y los jueces pasan a deliberar, en sesión secreta a la que solo podrá asistir el secretario, y sentenciar la causa, cerrando el debate.

Finalmente, se dará pronunciamiento a la sentencia en nombre de la República de El Salvador, al tenor de los requisitos establecidos (art. 395), no pudiendo dar esta por acreditados otros hechos u otras circunstancias que los descritos en la acusación y admitidos en el auto de apertura a juicio o, en su caso, en la ampliación de la acusación, salvo cuando favorezcan al imputado.

Distinguiéndose la sentencia en condenatoria o absolutoria, a través de las cuales de ordenarán las actuaciones que correspondan (art. 398 y 399).

Gráfico 5. *Proceso penal salvadoreño*. En este gráfico se muestra el proceso penal ordinario salvadoreño, aplicable también a la materia ciberdelictual.



Fuente: Elaboración propia

Tabla 2. *Cuadro comparativo de la regulación jurídica sustantiva en materia de ciberdelincuencia en los países de Nicaragua, Costa Rica y El Salvador.* En la siguiente tabla se evidencian contrastes entre la regulación jurídica sustantiva de Nicaragua, Costa Rica y El Salvador a razón de diversos elementos, tales como el ámbito de aplicación, el catálogo de ciberdelitos regulados o el objetivo perseguido por la norma.

	NICARAGUA	**COSTA RICA**	**EL SALVADOR**
Instrumento de regulación sustantiva	Ley 1042, Ley Especial de Ciberdelitos.	Código Penal.	Decreto No. 260, Ley Especial contra los delitos informáticos y conexos.
Terminología empleada	Delitos Cibernéticos/Informáticos (delitos relacionados con las TICs y los sistemas informáticos, cuya regulación se distingue por el fin, medio o método de comisión).	Delitos Informáticos y conexos (delitos relacionados con los sistemas informáticos cuya regulación es específica) y cibernéticos (delitos relacionados con las TICs cuya regulación se incluye como nueva modalidad de delitos tradicionales).	Delitos Informáticos y conexos (delitos relacionados con el uso de las tecnologías de la información y la comunicación y con los sistemas informáticos indistintamente).
Ámbito de aplicación	Será aplicable a todos los sujetos que cometan acciones, dentro o fuera del territorio nacional, utilizando los datos, sistemas informático o tecnologías de la información y la comunicación.	Se aplicará a quien cometa un hecho punible en el territorio de la República, salvo las excepciones establecidas en los tratados, convenios y reglas internacionales aceptados, incluyendo los hechos punibles cometidos en el extranjero regulados por el Código Penal.	Se aplicará a los hechos punibles cometidos total o parcialmente en el territorio nacional o en los lugares sometidos a su jurisdicción; también se aplicará a cualquier persona, natural o jurídica, nacional o extranjera, por delitos que afecten bienes jurídicos del Estado, de sus habitantes o protegidos por Pactos o Tratados Internacionales ratificados por El Salvador; incluyendo los actos cometidos en el extranjero de acuerdo a lo establecido en esta norma.
Objeto	Prevención, investigación, persecución y sanción de los delitos cometidos por	Prevenir y sancionar las acciones delictivas cometidas mediante el uso	Proteger los bienes jurídicos de aquellas conductas delictivas cometidas por medio de las

	medio de las Tecnologías de la Información y la Comunicación.	de las tecnologías de la información y la comunicación; y aquellas que involucren la utilización o que tengan como fin los sistemas informáticos.	Tecnologías de la Información y la Comunicación, así como su prevención y sancionamiento.
Tipologías delictivas	• **Ciberataques puros:** ○ Acceso indebido a los programas o datos informáticos. ○ Acceso indebido a sistemas informáticos. ○ Alteración, daño a la integridad y disponibilidad de datos. ○ Daño a sistemas informáticos. ○ Interceptación de comunicaciones y trasmisiones. ○ Interferencia del sistema informático o datos. ○ Violación de la seguridad del sistema informático. • **Ciberataques réplica:** ○ Acoso sexual. ○ Acoso. ○ Alteración, daño a la integridad y disponibilidad de datos. ○ Amenazas. ○ Captación indebida de comunicaciones ajenas. ○ Corrupción a personas	• **Ciberataques puros:** ○ Daño agravado. ○ Daño informático. ○ Instalación o propagación de programas informáticos maliciosos. ○ Instalación o propagación de programas informáticos maliciosos. ○ Suplantación de páginas electrónicas. • **Ciberataques réplicas:** ○ Acoso sexual en espacios públicos o de acceso público. ○ Amenaza a un funcionario público. ○ Corrupción de menores. ○ Difusión de información falsa. ○ Divulgación de información confidencial. ○ Espionaje informático. ○ Estafa informática. ○ Extorsión. ○ Facilitación de los medios para la	• **Ciberataques puros:** ○ Acceso Indebido a los Programas o Datos Informáticos. ○ Acceso Indebido a Sistemas Informáticos. ○ Alteración, Daño a la Integridad y Disponibilidad de los Datos. ○ Daños a Sistemas Informáticos. ○ Interceptación de Trasmisiones entre Sistemas de las Tecnologías de la Información y la Comunicación. ○ Interferencia de Datos. ○ Interferencia del Sistema Informático. ○ Secuestro de Sistemas, Programas o Datos Informáticos. ○ Violación de la Seguridad del Sistema. • **Ciberataques réplica:** ○ Acoso a Niñas, Niños y Adolescentes o Personas con Discapacidad.

	menores de 16 años o personas con discapacidad necesitada de especial protección. ○ Divulgación no autorizada. ○ Espionaje informático. ○ Falta a la confidencialidad. ○ Fraude informático. ○ Hurto por medios informáticos. ○ Manipulación de registros. ○ Manipulación fraudulenta de tarjetas inteligentes o instrumentos similares. ○ Obtención indebida de bienes o servicios por medio de tarjetas inteligentes o medios similares. ○ Posesión de equipos o prestación de servicios para vulnerar la seguridad informática. ○ Provisión indebida de bienes o servicios. ○ Provocación, apología e inducción a la comisión de delitos. ○ Revelación indebida de	consecución del delito informático. ○ Injurias. ○ Narcotráfico y crimen organizado. ○ Producción de material audiovisual. ○ Publicación de ofensas. ○ Sabotaje informático ○ Suplantación de identidad. ○ Trata de persona. ○ Turismo sexual. ○ Violación de correspondencia o comunicaciones. ○ Violación de datos personales. • **Ciberataques de contenido:** ○ Difusión de pornografía. ○ Fabricación, producción, o reproducción de pornografía. ○ Pornografía virtual y pseudo pornografía. ○ Tenencia de material pornográfico.	○ Acoso. ○ Corrupción de Niñas, Niños, Adolescentes o Personas con Discapacidad. ○ Espionaje Informático. ○ Estafa informática. ○ Extorsión sexual de niñas, niños y adolescentes o personas con discapacidad. ○ Falsedad de Documentos y Firmas. ○ Fraude Informático. ○ Hurto de Identidad. ○ Hurto por Medios Informáticos. ○ Manipulación de Registros. ○ Manipulación Fraudulenta de Tarjetas Inteligentes o Instrumentos Similares. ○ Obtención Indebida de bienes o servicios por medio de Tarjetas Inteligentes o Medios Similares. ○ Obtención y Divulgación No Autorizada. ○ Obtención y Transferencia de Información de Carácter Confidencial. ○ Posesión y uso de Equipos o Prestación de Servicios para la

	datos o información de carácter personal. ○ Suplantación informática. ○ Suplantación y apropiación de identidad informática. ○ Transferencia de información pública reservada. ○ Utilización de datos personales. ○ Violación de la custodia judicial de datos. • **Ciberataques de contenido:** ○ Propagación de noticias falsas. ○ Utilización de niñas, niños, adolescentes o personas con discapacidad necesitada de especial protección, en pornografía.		Vulneración de la Seguridad. ○ Provisión Indebida de Bienes o Servicios. ○ Revelación Indebida de Datos o Información de Carácter Personal. ○ Seducción de niñas, niños y adolescente o personas con discapacidad. ○ Técnicas de Denegación de Servicio. ○ Utilización de Datos Personales. • **Ciberataques de contenido:** ○ Adquisición o Posesión de Material Pornográfico de Niñas, Niños, Adolescentes o Personas con Discapacidad. ○ Intercambio de mensajes de contenido sexual con niñas, niños y adolescentes o personas con discapacidad. ○ Pornografía. ○ Utilización de Niñas, Niños, Adolescentes o Personas con Discapacidad en Pornografía.
	Penas privativas de libertad desde un año hasta diez años, las que	Penas privativas de libertad desde	

Consecuencias jurídicas	incluyen desde 100 días multa hasta 600 días multas como consecuencias accesorias; siendo la pena inferior de 200 a 300 días multa. Se regulan también agravantes comunes en casos determinados en donde la pena máxima será aplicada aumentada hasta en una tercera parte, junto con la inhabilitación del ejercicio de su profesión durante el tiempo que dure la pena.	seis meses hasta dieciséis años; siendo la pena mínima de diez a cincuenta días multa. Las penas se duplicarán cuando cualquiera de los delitos cometidos por medio de un sistema o red informática o telemática, o los contenedores electrónicos, ópticos o magnéticos afecte la lucha contra el narcotráfico o el crimen organizado.	Penas privativas de libertad desde un año hasta doce años; regulándose también agravantes comunes en casos determinados en donde la pena máxima será aplicada aumentada hasta en una tercera parte, junto con la inhabilitación del ejercicio de su profesión durante el tiempo que dure la pena.
Bienes jurídicos protegidos	Bines jurídicos individuales, colectivos y supraindividuales.	Bienes jurídicos individuales, colectivos y supraindividuales.	Bienes jurídicos individuales, colectivos y supraindividuales
Aspectos procesales	Medidas cautelares y procesales para la investigación, obtención y preservación de datos; e instrumentos de cooperación internacional. Riéndose en los demás de manera supletoria, por su Código Procesal Penal e instrumentos internacionales correspondientes.	Se rige por las disposiciones de su Código Procesal Penal e instrumentos internacionales en la materia.	No se establecen, rigiéndose por las disposiciones de su Código Procesal Penal, el cual fue reformado para la incorporación de apartados propios sobre delitos informáticos; e instrumentos internacionales en la materia.

Fuente: Elaboración propia

2. Análisis comparativo del régimen legislativo nicaragüense.

Ciertamente la normativización del cibercrimen ha representado un cambio significativo para la teoría del delito, introduciendo aspectos particulares que permiten su tipificación, mediante la explicación y aplicación de fenomenologías digitales, a razón de su complejidad, carácter, forma y modos de comisión.

Apreciándose claramente en la Ley No. 1042, Ley Especial de Ciberdelitos, del 27 de octubre de 2020, publicada en la Gaceta, Diario Oficial No. 201 del 30 de octubre

de 2020, el interés del Estado Nicaragüense de garantizar tanto la protección integral de los sistemas que utilicen de las TICs y sus componentes, como la protección de la persona, mediante la prevención, investigación, persecución y sanción del cibercrimen; estableciendo para ello diversos parámetros en atención de la acción, el sujeto, el resultado y su pena.

No obstante, en su afán por proteger pronto y eficazmente un bien jurídico dinámico, amplio, que exige de cambios sustanciales en las estructuras formales y materiales ya conocidas, ha cometido una serie de descuidos, que se ven reflejados en su ámbito de aplicación y consecuentemente en su contenido, a raíz de la no previsión de los requerimientos de calidad técnico formal, incurriendo en defectos iterativos, ya previstos anteriormente por legislaciones similares.

Como en su momento se advirtió a El Salvador, sobre el anteproyecto de Ley Especial contra Delitos Informáticos y Conexos, preparado y presentado en abril del 2015; señalando que una ley especial debería limitarse a incluir aquellos delitos propiamente informáticos y no aquellos que utilicen a las TIC como un medio o que se trate de una misma conducta delictiva realizada en el ciberespacio, distinguiendo los delitos comunes que son realizados por medio de sistemas informáticos o telemáticos, de los cibercrímenes; constando además con una descripción clara que permita distinguir una conducta de otra, de forma que no conduzca hacia una doble tipificación y consecuentemente al error en la aplicación de la ley.

En el mismo sentido Costa Rica, siguiendo estos lineamientos y a través de su última reforma del año 2012, modificó ciertos de sus artículos para incluir dentro de ellos la modalidad de comisión a través del uso de las TICs, e incorporando diferenciadamente otros delitos relacionados con los medios informáticos.

Por otro lado, en el caso específico de Nicaragua, podemos observar desde su art. 2 LEC la carente determinación de su ámbito de aplicación, señalando, sin mayor detalle que la ley se aplicará “dentro o fuera del territorio nacional”.

Lo que, inevitablemente, exige recurrir de forma supletoria al Código Penal, el cual, del artículo 13 al 16 dispone el ámbito de aplicación de las leyes penales nicaragüenses.

En el caso de Costa Rica, el ámbito de aplicación para los ciberdelitos se rige por las disposiciones generales de delitos tradicionales reguladas en el artículo 5, 6, 6 bis y 7 sobre territorialidad, extraterritorialidad, hechos punibles cometidos en el extranjero, actos de terrorismo y delitos internacionales.

A diferencia de El Salvador, que en su art. 2 LEDIC, enfatiza que se aplicará a hechos punibles cometidos total o parcialmente en el territorio nacional o en los lugares sometidos a su jurisdicción; cualquier persona, natural o jurídica, nacional o extranjera, por delitos que afecten bienes jurídicos del Estado, de sus habitantes o protegidos por Pactos o Tratados Internacionales ratificados por El Salvador; la ejecución del hecho que se inició en territorio extranjero y se consumó en territorio nacional; o si se hubieren realizado, utilizando Tecnologías de la Información y la Comunicación instaladas en el territorio nacional y el responsable no ha sido juzgado por el mismo hecho por tribunales extranjeros o ha evadido el juzgamiento o la condena.

Por otro lado, en cuanto a la regulación de la responsabilidad penal de las personas jurídicas ante la comisión de un ciberdelito, Costa Rica es el único país de los estudiados en contemplarlo, esto a través de la ley 9699 del año 2019 la cual sanciona delitos contemplados en la Ley contra la Corrupción y el Enriquecimiento Ilícito en la Función Pública, y en el Código Penal.

Este tema de la responsabilidad penal de las personas jurídicas es el resultado de un fenómeno denominado «modernización del derecho penal», teniendo su origen, en Italia y en los demás países europeos, en el desarrollo de la criminalidad y, en consecuencia, de los modelos de control social penal.[115] Se trata, además, de un desarrollo previsible del paso de la sociedad moderna de simple a compleja.

115. PALIERO, Carlo. “Problemas y perspectivas de la responsabilidad penal de la persona jurídica en el derecho penal italiano”. En: “*Responsabilidad penal de las personas jurídicas”*.

Modernización que se ha implicado también en la materia ciberdelincuencial a razón del crecimiento de las nuevas tecnologías y el acceso a Internet, lo que se ha traducido en un incremento en el riesgo de exposición de las organizaciones a determinados delitos en donde encuentra mayor relevancia la seguridad de la información en el contexto empresarial.

A pesar de esto, se sigue cuestionando bastante la posibilidad de responsabilizar penalmente de modo autónomo y directo a las agrupaciones respecto a la amplia esfera de actividades ilegales en la que operan como autores en sentido propio y estricto; de manera tal que el debate, principalmente doctrinal, sobre la responsabilidad penal de personas jurídicas ha sido y es hasta ahora bastante intenso. Este debate no es excluyente en materia ciberdelictual, es más, podría decirse que se vuelve aún más complicado.

En cualquier caso, se han ido desarrollado en la actualidad diversos modelos que buscan precisamente hacer frente a esas dificultades que impiden el sancionamiento de las personas jurídicas, fundamentados en las siguientes consideraciones:

- La dificultad para exigir responsabilidades individuales en el seno de empresas complejas con tendencia a tener una responsabilidad diseminada.
- Un escaso efecto preventivo en la organización de la responsabilidad individual o de la propia del derecho administrativo sancionador.
- Vinculación de la responsabilidad penal con la promoción de la autorregulación en la esfera empresarial a través de los *Compliance Programs.*[116]
- Eliminación de lagunas punitivas y minimización los previsibles intentos de desplazamiento de la carga desde la persona jurídica a la física, y al revés.

Coord. HURTADO, José. España: Grijley, 1997, p. 47. [En línea] [Consultado el 20 de julio de 2022]. Disponible en: https://perso.unifr.ch/derechopenal/assets/files/anuario/an_1996_05.pdf

116. MAÑAS, Vanessa. *Responsabilidad penal corporativa y cibercriminalidad. El compliance penal relativo al Derecho de las TIC* [En línea]. Trabajo de grado. Universidad de Barcelona, 2017, p. 41 [Consultado el 24 de julio de 2022]. Disponible en: http://diposit.ub.edu/dspace/bitstream/2445/119488/1/TFG%20%20Vanessa%20Ma%C3%B1as.pdf

En otro orden de ideas, dentro del texto normativo de la Ley 1042, Ley Especial de Ciberdelitos, es posible visualizar en varios artículos una carencia en la técnica legislativa utilizada. Por ejemplo:

El artículo 8 sobre interferencia del sistema informático o datos dispone textualmente que: *El que intencionalmente y por cualquier medio interfiera o altere el funcionamiento de un sistema informático…*Con lo cual, no aclara si el sistema informático está bajo la propiedad o facultad legal de disposición del autor. De hecho, en las definiciones hechas por la misma Ley Especial de Ciberdelitos, sobre "Interceptación", no hace referencia alguna a acción ilegitima (art. 3. 14); pues efectivamente la simple interceptación intencionada o no, no constituye una acción delictiva sin el elemento de ilegitimidad.

Mismo problema se identifica en el caso de El Salvador, cuya descripción de la acción en el artículo 6 es prácticamente igual, limitándose al establecimiento de la intencionalidad.

En el contexto costarricense, la referida acción es sancionada a través del artículo 229 *ter* sobre sabotaje informático, el cual sí incluye la condición de falta de autorización.

De nuevo en el contexto nicaragüense, se puede observar en el artículo 10 la falta de determinación sobre la conducta del sujeto activo, pues no se considera la legitimidad o no de la acción, señalando únicamente: *El que destruya, dañe, modifique, ejecute un programa o realice cualquier acto que altere el funcionamiento o inhabilite parcial o totalmente un sistema informático…*

Nuevamente, la descripción que hace El Salvador a dicha conducta sobre daño a sistemas informáticos a través del artículo 7, es análoga.

En el caso de Costa Rica este problema no se presenta, pues en su artículo 229 *bis* sobre daño informático establece claramente la concurrencia de la acción sin autorización o excediendo la que se haya otorgado.

En los artículos referidos, el elemento circunstancial es la falta de definición de la *ilegitimidad* de la acción, cuestión que ya la Convención del Consejo de Europa

sobre la Delincuencia Cibernética[117] e incluso el Convenio de Budapest contemplan como la forma adecuada de tipificar las conductas.

Estas ambigüedades solo generan inseguridad jurídica y el legislador debe siempre procurar la claridad y no la creación de situaciones confusas, argumentos que resaltan la falta de aplicación de una depurada técnica legislativa –no la criminalización de una acción no delictiva— viéndose afectados tanto víctimas potenciales, como viables acusados.

Situación similar a las ya referidas se puede identificar en el artículo 26 sobre Revelación indebida de datos o información de carácter personal el cual señala que: *El que, sin el consentimiento del titular de la información de carácter privado y personal, revele, difunda o ceda en todo o en parte, dicha información o datos*…En este caso, la norma no define si el autor obtuvo la información, datos o contenido de manera legitima o no, en cuyo caso la acción podría perfectamente encasillarse en el artículo 195 del Código Penal sobre Propalación el cual señala textualmente: *Quien hallándose legítimamente en posesión de una comunicación, de documentos o grabaciones de carácter privado, los haga públicos sin la debida autorización…* Por lo que, para no caer en una doble tipificación, la ley 1042 debe establecer inequívocamente en el artículo 26 la revelación de datos o información obtenida ilegítimamente.

En cualquiera de los casos, somos conscientes que en la práctica se aplica el delito de propalación cuando la obtención es legítima y el delito de revelación indebida cuando la obtención es ilegítima; no obstante, no está de más mencionar la confusión que puede llegar a generar la falta de determinación de legitimación en el artículo 26.

117. Departamento de cooperación jurídica. Legislación sustantiva de delito cibernético. [En línea] [Consultado el 24 de julio de 2022]. Disponible en: http://www.oas.org/juridico/spanish/cybersp_legis.htm

Siguiendo con la falta de claridad puede hacerse mención también del artículo 21 sobre falta de confidencialidad, el cual textualmente señala que: *Quien faltare a la confidencialidad sobre la información que conoció…*

En este artículo se evidencia nuevamente una falta de determinación de las acciones que pueden llevar a "faltar a la confidencialidad", pues en efecto, este tipo delictivo puede envolver dentro de sí un sinfín de acciones que perfectamente pueden ser enmarcadas en otras tipologías, por ejemplo, en el artículo 26 sobre Revelación indebida de datos o información de carácter personal; muestra clara de una falta de confidencialidad.

Este problema no se presenta ni en El Salvador ni en Costa Rica, precisamente porque dicha conducta de "falta a la confidencialidad" se ve regulada a través de otros tipos delictivos.

Haciendo referencia ahora al controversial artículo 30, se tocarán algunas de las dificultades que se han podido observar.

En primer lugar, el artículo 30 no define lo que se entenderá como "noticias falsas" para efectos de comisión delictiva, pudiendo entenderse que la simple difusión de la misma es un acto delictivo, cuando en efecto no es así; toda acción exige de relevancia penal para ser considerada como delictiva.

La relevancia penal implica que se produzca afectación a bienes jurídicos, pues en efecto, las noticias falsas pueden ser de tan variado contenido que, dependiendo de a qué se refieran y con qué intención sean difundidas, pueden llegar a integrar muy diferentes tipos penales como los delitos de odio, descubrimiento y revelación de secretos, delitos contra la integridad moral, desórdenes públicos, injurias y calumnias, delitos contra la salud pública, delitos contra el mercado y los consumidores, etc.

Al respecto, el referido artículo si establece los casos en la acción será motivo de castigo, por ejemplo: cuando incite al odio y a la violencia, pone en peligro la estabilidad económica; no obstante, dichas circunstancias se ven revestidas de

subjetividad y amplia discrecionalidad ya que no se establecen los parámetros específicos para establecer dichos efectos sociológicos, o bien, tampoco se definen.

Todo esto genera una vez más inseguridad jurídica y la posibilidad de afectación de bienes jurídicos como perfectamente podría ser el derecho a la libertad de expresión, a razón de una carente articulación, lo que puede generar una deficiente aplicación como consecuencia de una incorrecta interpretación.

En el contexto salvadoreño la acción de difusión de noticias falsas o tergiversadas no es prevista.

Mientras que, en el caso de Costa Rica, su artículo 236 además de no definir la noción de noticias falsas e incluir situaciones bastante subjetivas –al igual que Nicaragua— se limita a su sancionamiento cuando las mismas provoquen perjuicio a la seguridad y estabilidad del sistema financiero o de sus usuarios. Dejando fuera de regulación otros bienes jurídicos como los ya referidos anteriormente que también ameritan protección.

Desde otra perspectiva, se observan también en el contexto nicaragüense ciertas dificultades relativas a la limitación de comisión delictiva por parte de personas mayores de edad, ejemplo de ello es el artículo 32, el cual señala que: *Toda persona mayor de 18 años que haga propuestas implícitas o explícitas a personas menores de 16 años o personas con discapacidad necesitada de especial protección…*

Mismo problema se observa en el caso del ciberacoso sexual regulado en el artículo 34, el cual señala que: *Cuando una persona mayor de edad, envíe mensajes, frases, fotografías, vídeos u otra acción inequívoca de naturaleza o contenido sexual a otra persona sin su consentimiento…*

En estos artículos se expresa claramente como único sujeto activo a las personas mayores de edad, excluyendo la posibilidad de que la comisión del referido delito pueda ejecutarse por un menor de edad. Pues si bien es cierto el artículo 33 del Código Penal exime de responsabilidad penal a aquellos menores de dieciocho años, señala también que si la acción delictiva es realizada por un adolescente –entiéndase adolescente como aquellas personas que está entre los 10 y 19 años de

edad[118]– podrá responsabilizarse de acuerdo a lo dispuesto en el Libro Tercero, Sistema de Justicia Penal Especializada del Código de la Niñez y la Adolescencia.

Por lo que, la ley Especial de Ciberdelitos debería ser clara en cuanto a la responsabilidad en la que puede incurrir un menor de edad al cometer alguna de estas acciones, pues desde el momento en que se limita a mencionar a personas "mayores de edad", se excluye en teoría la posibilidad de aplicar las disposiciones del artículo 95 del referido código de la niñez y adolescencia.

En el caso de El Salvador, no se dispone en ninguno de los tipos penales alguna restricción de edad para la comisión de los mismos, posibilitando el sancionamiento de los menores de edad de acuerdo a las normas correspondientes.

Misma situación se presenta en el caso de Costa Rica; aunque aquí el problema sería relativo a la falta de regulación del ciberacoso o ciberacoso sexual; lo único que existe hasta el momento sobre esto es el proyecto de ley № 21.507 llamado "Ley del Grooming", siendo las únicas conductas sancionadas actualmente en el código penal la corrupción de menores en el artículo 167.

Así, en los párrafos anteriores se evidenció una gran cantidad de deficiencias principalmente de tipo técnico, no obstante, otro problema que merece atención es la percepción social negativa que se tiene de la norma.

Para nadie es sorpresa que la ley 1042 ha sido objeto hasta el día de hoy de innumerables críticas y debates, las cuales se centran principalmente en atacar la legitimidad de la misma, es decir, su justicia o los juicios de valores que la envuelven, sin embargo, nuestro estudio no ha demostrado la injusticia de la norma— al menos no desde el texto jurídico—, pero definitivamente, siendo conscientes de la negativa existente, adentrarse en el estudio práctico de las

118. UNICEF. ¿Qué es la adolescencia? [En línea] [Consultado el 20 de julio de 2022]. Disponible en: https://www.unicef.org/uruguay/que-es-la-adolescencia#:~:text=La%20Organizaci%C3%B3n%20Mundial%20de%20la,los%2010%20y%2019%20a%C3%B1os.

percepción social es indispensable para identificar las razones de la misma a fin de diseñar planes y estrategias que den lugar a su solvencia.

3. Regulación Jurídica internacional.

3.1. Convenio Iberoamericano de cooperación sobre investigación, aseguramiento y obtención de prueba en materia de ciberdelincuencia.[119] (Nicaragua).

El presente convenio del año 2014, tal como el mismo lo describe, tiene como finalidad dotar a los países del ámbito iberoamericano de una herramienta que facilite lo que resulte fundamental en la lucha contra el ciberdelito que es la Cooperación entre ellos, considerando que las nuevas modalidades delictivas producto de los avances tecnológicos que traspasan fronteras y dificultan su persecución, exigen de instrumentos capaces de actuar con celeridad para no perder pruebas, e incluso prevenir y evitar daños.

Este convenio procura la cooperación judicial entre los Estados partes a través de la adopción de medidas que permitan el aseguramiento y obtención de pruebas en materia de ciberdelincuencia, proceso que se llevará a cabo por medio de solitudes por una u otras partes, pudiendo el país requerido negarse al requerimiento en los casos previstos, negativa que deberá ser debidamente razonada (art. 1-3)

Las solicitudes versaran sobre las medidas de aseguramiento y diligencias de investigación establecidas en el Convenio (art. 6-7), entre las cuales están la incautación de depósitos de sistemas informáticos, preservación inmediata de datos, acceso a sistemas de información, entre otras.

119. Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de prueba en materia de Ciberdelincuencia, hecho en Madrid, el día 28 de mayo de 2014. Aprobado por Nicaragua, a través del DECRETO A.N. No. 8651 del 25 de febrero de 2020, publicado en La Gaceta – Diario Oficial, No. 42, del 03 de marzo de 2020 y ratificado mediante DECRETO PRESIDENCIAL No. 08-2020 del 16 de abril de 2020, publicado en La Gaceta – Diario Oficial, No. 73 del 24 de abril de 2020.

Para la procedencia de las solicitudes se deberán cumplir los requisitos correspondientes (art. 9) en donde se incluyen:

- Autoridad competente.
- Hechos.
- Calificación jurídica.
- Preceptos legales.
- Objetivo de la solicitud y condiciones de la misma.

Hecho esto la solicitud se tramitará de acuerdo al procedimiento determinado (art. 10), pudiendo ser rechazada total o parcialmente, devuelta, aceptada o aceptada de forma condicionada; si la solicitud es admitida se le dará cumplimiento.

Para estos efectos, los Estados se comprometen a realizar las iniciativas legislativas necesarias en su normativización interna que permitan la ejecución de las solicitudes, estableciéndose las autoridades que se encargarán de su envío y recepción, designándose también al menos un punto de contacto disponible todos los días del año y durante las 24 horas del día (art. 8). Estas autoridades serán designadas al momento de la ratificación del presente Convenio y podrán ser sustituidas en cualquier momento (art. 13).

3.2. Tratado de asistencia legal mutua en asuntos penales entre las repúblicas de El Salvador, Guatemala, Honduras, Nicaragua, Costa Rica y Panamá.[120] (Nicaragua, El Salvador, Costa Rica).

El Tratado de asistencia penal mutua fue suscrito en el año 1993, y tiene como objetivo la cooperación legal en asuntos penales relacionados con cualquier hecho

120. Tratado de asistencia legal mutua en asuntos penales entre las repúblicas de El Salvador, Guatemala, Honduras, Nicaragua, Costa Rica y Panamá, hecho en Guatemala, el día 29 de octubre de 1993. Aprobado por Nicaragua, a través del DECRETO A.N. No. 1902 del 11 de junio de 1998, publicado en La Gaceta – Diario Oficial, No. 116, del 23 de junio de 1998 y ratificado mediante DECRETO PRESIDENCIAL No. 40-99 del 24 de marzo de 1999, publicado en La Gaceta – Diario Oficial, No. 68 del 14 de abril de 1999.

punible tipificado como tal tanto en el Estado requirente como en el Estado requerido (art. 2).

Esta asistencia o cooperación incluye la obtención y ejecución de pruebas, la localización de personas, la ejecución de medidas cautelares, incluyendo la recepción de testimonios de personas que se encuentran en el país requerido, suministro de copias de documentos públicos, entre otras cosas, para lo cual el tratado establece el procedimiento que deberá seguirse y los plazos que deban respetarse para cada caso (art. 3, 7-17).

Asimismo, se establecen excepciones sobre las cuales no se podrá solicitar asistencia, por ejemplo, en casos de extradición, impuestos, transferencia de procesos penales y todas aquellas señaladas en el tratado.

Las autoridades encargadas de recibir y tramitar las solicitudes varían en dependencia de cada país, pero para los países que nos son de interés, las autoridades competentes son:

- **Nicaragua:** La Procuraduría General de Justicia.
- **Costa Rica:** La Procuraduría General de la República
- **El Salvador:** La Corte Suprema de Justicia.

Toda solicitud de asistencia deberá cumplir con una serie de requisitos formales (art. 4), si se cumplen con todos ellos, la Autoridad Central del Estado Requerido deberá cumplir prontamente con la solicitud a través de todos los medios legales a su alcance (art. 5).

No obstante, hay excepciones al cumplimiento de la solicitud de asistencia, cuando, por ejemplo, la solicitud de asistencia se refiere a un delito político o se refiere a un delito que no está tipificado como tal en el Estado Requerido (art. 6)

Los costos derivados de la solicitud serán asumidos por el Estado requirente, esto incluye, honorarios, gastos de viaje, gastos de traducción, entre otros, a excepción de aquellos gastos realizados por el Estado requerido dentro de su territorio para el cumplimiento de la solicitud, menos aquellos que, previo acuerdo, le correspondan al Estado requirente (art. 18)

Finalmente, toda la información que sea proporcionada por el Estado requirente solo podrá ser utilizada para los fines establecidos en la solicitud sin previo consentimiento del Estado requerido. Asimismo, toda esta información se mantendrá en estricta confidencialidad, salvo que éstas sean requeridas en investigaciones que formen parte de un proceso penal descrito en la solicitud de asistencia (art. 19-20)

3.3. Convención Interamericana sobre asistencia mutua en materia penal. [121] (Nicaragua, El Salvador, Costa Rica).

Esta Convención del año 1992, tiene como prepósito la asistencia legal mutua en materia penal, al igual que el anterior Tratado De Asistencia Mutua En Materia Penal, sobre investigaciones, juicios y actuaciones referentes a delitos cuyo conocimiento sea de competencia del Estado requirente al momento de solicitarse la asistencia (art. 1-2).

En este caso no se establece una autoridad central como tal para cada Estado, sino que se señala que cada uno de ellos se encargará de su designación para efectos de envío y recibimiento de solicitudes de asistencia (art. 3).

Es ineludible, que el hecho por el que se solicita asistencia, sea punible tanto en el país requerido como en el requirente, a excepción de los casos establecidos en el Convenio (art. 5), y sea punible con pena de un año o más de prisión en el Estado requirente (art. 6).

Esta solicitud podrá versar sobre cualquiera de los actos previstos en el Convenio y de acuerdo a los procedimientos específicos ya establecidos para cada caso concreto (art. 7); exceptuándose los casos sobre delitos militares, políticos, tributarios, o cualquier otro que ya el instrumento señala (art. 8-9)

121. Convención Interamericana sobre Asistencia Mutua en Materia Penal, hecha en Bahamas, el día 23 de mayo de 1992. Aprobado y ratificado por Nicaragua, a través del DECRETO PRESIDENCIAL No. 77-2002 del 29 de agosto de 2002, publicado en La Gaceta – Diario Oficial, No. 173, del 12 de septiembre del 2002.

De igual manera las solicitudes, serán elaboradas de acuerdo a la legislación interna de cada país, mientras no contravenga con la del país requerido, cumpliendo este los trámites de la solicitud, pudiendo postergarlo con explicación de causa cuando sea necesario. Sin embargo, las solicitudes deberán contener las indicaciones sobre el acto que origina la solicitud, descripción de los hechos, delito a que se refiere, descripción de la asistencia que se requiere, entre otras cosas (art. 26).

Los gastos ordinarios dentro del Estado requerido estarán a su cargo a excepción de los casos previsto en el Convenio (art. 29). Y en caso de algún daño derivado de los actos ejecutados, será la ley interna de cada país la que establezca la responsabilidad correspondiente (art. 31).

3.4. Convención de las Naciones Unidas contra la delincuencia organizada Transnacional.[122] (Nicaragua, El Salvador).

La CDOT, suscrita en Palermo (Italia), durante diciembre del año 2000, enmarco un hito para el fortalecimiento de la lucha contra la delincuencia organizada; donde el manifiesto de la voluntad política, tras la comprensión global de la delincuencia organizada trasnacional como problemática mundial, demostró el interés de la comunidad internacional por responder a los desafíos globales de la aplicación de la ley, para la defensa de los derechos humanos y la erradicación de la delincuencia, la corrupción y la trata de personas.

Concretando dichos esfuerzos tras la materialización de un nuevo instrumento, propicio, para el afrontamiento de la delincuencia como problemática mundial, fortaleciendo, consecuentemente, la cooperación internacional, con el interés de potenciar la actuación eficaz de la acción de la ley, en los planos nacional, regional

122. Convenio de las Naciones Unidas contra la Delincuencia Organizada Transnacional, hecho en Italia, el día 14 de diciembre del 2000. Aprobado por Nicaragua, a través del DECRETO A.N. No. 3246 del 13 de febrero de 2002, publicado en La Gaceta – Diario Oficial, No. 38, del 25 de febrero de 2002 y ratificado mediante DECRETO PRESIDENCIAL No. 62-2002 del 18 de junio de 2002, publicado en La Gaceta – Diario Oficial, No. 121 del 28 de junio de 2002.

e internacional, de modo que permita salvaguardar la seguridad y dignidad de sus comunidades.[123]

Siendo este su propósito, el cual consiste, conforme mandata su art. 1, en: "Promover la cooperación para prevenir y combatir más eficazmente la delincuencia organizada transnacional".

Manifestando además su alto respeto hacia los principios de igualdad soberana, integridad territorial y no intervención, como una fuente de resguardo a la importancia de la soberanía estatal, como expresamente advierte en su art. 4 que:

- Los Estados Parte cumplirán sus obligaciones con arreglo a la presente Convención en consonancia con los principios de igualdad soberana e integridad territorial de los Estados, así como de no intervención en los asuntos internos de otros Estados.
- Nada de lo dispuesto en la presente Convención facultará a un Estado Parte para ejercer, en el territorio de otro Estado, jurisdicción o funciones que el derecho interno de ese Estado reserve exclusivamente a sus autoridades.

No obstante, a pesar de sus bonanzas para la homogeneización normativa, dicho instrumento ha sido, a lo largo de sus 22 años de vigencia, criticado por no permitir per se el ejercicio de la jurisdicción penal extraterritorial para juzgar crímenes transnacionales, dado que no concede a los tribunales nacionales de los estados partes la capacidad de investigar, procesar y sancionar a presuntos autores de delitos cometidos fuera de su territorio. Por lo que se le acusa de insustancial e inefectivo contra el crimen organizado transnacional. [124]

123. UNODC. Convención de las Naciones Unidas contra la delincuencia organizada transnacional y sus protocolos [En línea]. Nueva York: Naciones Unidas, 2004, pp. 5-12. [Consultado el 10 de junio de 2022]. Disponible en: https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-s.pdf

124. Diálogo de Derechos Humanos. La Convención de las Naciones Unidas Contra la Delincuencia Organizada Transnacional. [En línea] [Consultado el 21 de junio de 2022]. Disponible en: https://dialogoderechoshumanos.com/blog/614-la-convencion-de-las-naciones-unidas-contra-la-delincuencia-organizada-transnacional

Además, como se puede apreciar en reiteradas ocasiones, que la norma traslada la problemática de la jurisdicción expresamente a los estados parte, señalando que: ¨Cada Estado parte adoptará las medidas que sean necesarias para establecer su jurisdicción respecto a los delitos tipificados en la presente convención…¨ como podremos apreciar en los artos. 5, 6, 7, 8, 9, 10, 11, 15, 24, 20, 23, 25, 27 y 34.

Estableciendo sucesivamente una serie de supuestos de hecho, en los que los distintos Estados miembros podrían promulgar normas que permitan a sus tribunales nacionales el enjuiciamiento de determinadas categorías de crímenes transnacionales cometidos más allá de sus fronteras, indicando en el art. 15, que procederá cuando:

- Cuando el delito se cometa contra uno de sus nacionales.
- Cuando el delito sea cometido por uno de sus nacionales o por una persona apátrida que tenga residencia habitual en su territorio.
- La participación en un grupo delictivo en el extranjero, con miras a cometer un delito grave dentro del territorio nacional.
- En los casos de blanqueo dentro del territorio nacional, del producto del delito cometido en el extranjero.

Lo que encauza al Estado que juzgue de un delito transnacional cometido fuera de su territorio a la revisión primaria de la legislación interna de dicho Estado, pasando a secundario la CDOT, para determinar si la misma atribuye a sus tribunales nacionales, el poder de investigar y procesar a presuntos autores de delitos cometidos en el extranjero. [125]

Sin embargo, eso no significa que la misma no haya efectuado importantes aportes a la lucha contra el crimen organizado trasnacional, de los que podemos destacar:

- **La definición de aceptación universal, de conceptos esenciales e inherentes a la delincuencia organizada transnacional:** La CDOT establece el marco conceptual y legal necesario para la concreción de la cooperación internacional y el consecuente aumento de posibilidades de éxito contra la

125. Ibídem

delincuencia organizada transnacional; logrando en consenso de definiciones legales esenciales dentro de la comunidad internacional, para la facilitación de la colaboración y asistencia recíproca entre las naciones, garantizando el correcto entendimiento del crimen organizado transnacional. Señalando, en su art. 2, para fines de la convención, conceptos como:

  - **Grupo delictivo organizado:** Un grupo estructurado de tres o más personas que exista durante cierto tiempo y que actúe concertadamente con el propósito de cometer uno o más delitos graves o delitos tipificados por la Convención, con miras a obtener, directa o indirectamente, un beneficio económico u otro beneficio de orden material.
  - **Delito grave:** Conducta que constituya un delito punible con una privación de libertad máxima de al menos cuatro años o con una pena más grave.
  - **Producto del delito:** Bienes de cualquier índole derivados u obtenidos directa o indirectamente de la comisión de un delito.
  - **Entre otros.**

- **El acercamiento entre las diversas legislaciones penales**: La ratificación de la CDOT instituye a los Estados partes el compromiso de armonizar sus legislaciones internas, acorde a las definiciones conceptuales contenidas, así como la adecuación de sus penas.
- **La fijación de compromisos, pautas y procedimientos para la asistencia técnica y cooperación internacional:** Bajo el entendido de que la acción integrada de la comunidad internacional resulta crucial para descubrir, investigar y enjuiciar a personas y grupos responsables de crímenes transnacionales, la CDOT crea estándares de actuación, protocolos y procedimientos para la asistencia judicial y la cooperación multilateral, incluida la extradición, todo bajo un marco de respeto a la soberanía de cada uno de los Estados partes. [126]Como ampliamente observaremos a lo largo de su artículo 18.

126. Ibídem

3.5. Convenio de Budapest.[127] (Costa Rica).

El Convenio de Budapest del año 2001 tiene como objetivo hacer efectiva la lucha contra el cibercrimen por medio de la armonización de las legislaciones dedicadas a esta materia.

En cuanto a la estructura del Convenio, éste consta de 48 artículos y un preámbulo inicial. En concreto se establecen hasta cuatro capítulos, divididos en secciones y títulos. El primer capítulo tan sólo comprende un precepto, referido a la terminología usada en el texto. El capítulo segundo «Medidas que deberán adoptarse a nivel nacional», incluye elementos tanto de Derecho material (responsabilidad penal, tentativa, complicidad...) como procesal (procedimiento, salvaguardas, datos, registros, jurisdicción…). En cuanto al tercero, se introduce directamente en la cooperación internacional. Abarca cuestiones como la extradición, la asistencia entre Estados, la información, el intercambio de datos y el establecimiento de una red 24/7. El último capítulo contiene las disposiciones finales propias de un Tratado internacional: adhesión, entrada en vigor, aplicación territorial, efectos, régimen de reservas, denuncias, notificaciones, etc.

En el segmento sobre derecho penal sustantivo, el presente instrumento expone un listado de tipos penales que deberán ser adoptados por los Estados partes en sus normas internas, los cuales a su vez se dividen en cinco categorías:

- **Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos (art. 2-6):**
    - Acceso ilícito.
    - Interceptación ilícita.
    - Ataques a la integridad de los datos.
    - Ataques a la integridad de los sistemas.
    - Abuso de los dispositivos.
- **Delitos informáticos (art. 7-8):**

127. Convenio sobre la ciberdelincuencia, hecho en Budapest, el día 23 de noviembre de 2001. Nicaragua no es firmante, sin embargo, toma en consideración la parte sustantiva de dicha norma en la Ley Nº. 1042.

- Falsificación informática.
- Fraude informático.

- **Delitos relacionados con el contenido (art. 9):**
  - Delitos relacionados con la pornografía infantil.
- **Delitos relacionados con infracciones de la propiedad intelectual y de los derechos a fines (art. 10):**
  - Delitos relacionados con infracciones de la propiedad intelectual y de los derechos a fines.
- **Otras formas de responsabilidad y sanción (art. 11-13):**
  - Tentativa y complicidad.
  - Responsabilidad de las personas jurídicas.
  - Sanciones y medidas.

Por otra parte, en lo que respecta al apartado sobre derecho penal procesal, el convenio establece una serie de presupuestos procesales, indicando, en primer lugar, que cada Estado parte deberá adoptar las medidas legislativas que considere necesarias para:

- **El establecimiento de los poderes y procedimientos (art. 14-15):** Correspondientes los cuales serán aplicados a:
  - Los delitos estipulados en el Convenio (art. 2-11).
  - Cualquier otro delito cometido por medio de un sistema informático.
  - La obtención de pruebas electrónicas.

  Estos poderes y procedimientos deberán estar sujetos a condiciones y salvaguarda de acuerdo a cada derecho interno, las cuales podrán incluir, según sea el caso, supervisión judicial u independiente, justificación de aplicación, limitaciones de aplicación y duración.

  Cada Estado parte se encargará de examinar los efectos de los poderes y procedimientos cuando sea de interés público y de acuerdo a la buena administración de la justicia.
- **La conservación rápida de datos informáticos almacenados (art. 16)**: Principalmente cuando sean susceptibles de pérdida o modificación. Si se ordena la conservación de los datos al sujeto que los tiene en su poder o bajo

su control, se podrán adoptar las medidas necesarias para obligarlo a dicho fin hasta por 90 días, pudiendo la orden ser renovada. Dicha orden podrá incluir la obligación de mantener en secreto la ejecución de dichos procedimientos durante el tiempo que se prevea en el derecho interno.

- **La conservación y revelación parcial rápida de datos relativos al tráfico (art. 17):** Con el objetivo de garantizar la conservación rápida de los datos; revelación rápida de los datos a autoridad competente o designada y obtención de información necesaria que permita identificar a los proveedores de servicios y las vías por las que la comunicación ser ha transmitido.
- **La orden de presentación (art. 18):** Se refiere a la orden para obligar a una persona dentro del territorio y/o a un proveedor que ofrezca sus servicios dentro del mismo a que comunique determinados datos informáticos que se encuentren en su poder o bajo su control, en este último caso, relativos a los abonados en relación con dicho servicio.
- **El registro y confiscación de datos informáticos almacenados (art. 19):** Esto para facultar a sus autoridades a registrar o tener acceso a:
    - Sistemas informáticos y datos en el almacenado.
    - Dispositivos de almacenamiento informático.

  Y, en caso de que las autoridades consideren que los datos buscados se encuentran en otro sistema informático o en otra parte del mismo, o que sean legítimamente accesibles o disponibles por medio del sistema inicial, puedan extender rápidamente el registro o acceso.

  Una vez que se logre acceder a los datos, cada estado aplicará las medidas necesitar para proceder a su obtención o confiscación.

  En todo caso, los estados podrán ordenar a toda persona que tenga conocimiento sobre sistemas informáticos a que proporcione la información necesaria para permitir el registro, acceso y confiscación dentro de lo razonable.
- **La obtención en tiempo real de datos relativos al tráfico (art. 20):** Las medidas deben facultar a las autoridades competentes a obtener o grabar con medios técnicos y en tiempo real, los datos relativos al tráfico asociados a

comunicaciones especificas trasmitidas en el territorio por medio de un sistema informático.

De no ser posible, se deberá ordenar a cualquier proveedor de servicios a obtener o grabar con medios electrónicos o a ofrecer a las autoridades su colaboración y asistencia para obtener y grabar. En este caso se practicarán las medidas necesarias que permitan mantener en secreto el hecho y la información que se obtenga.

De no poder dar cumplimiento a esta disposición a razón de legislación interna, el Estado podrá reservarse el derecho a su práctica, aplicando en cambio otras medidas que permitan el mismo fin.

- **La intercepción de datos relativos al contenido (art. 21):** Las medidas deben facultar a las autoridades competentes en lo que respecta a un repertorio de delitos graves, el cual se dirigirá a la obtención o grabación, tal como lo dispone el apartado anterior y de acuerdo a los mismos preceptos y fines.
- **Afirmar su jurisdicción (art. 22):** Esto respecto de cualquiera de los delitos referidos en este Convenio, cuando sea cometido en:
    - Su territorio.
    - En un buque que enarbole su pabellón.
    - En una aeronave matriculada según las normas internas.
    - Otro Estado por uno de sus nacionales en los casos previstos en este instrumento.

  Los Estados partes podrán reservarse su derecho a aplicar medidas de jurisdicción o aplicarlas solo en casos determinados.

  No se excluye la jurisdicción penal que pueda ser ejercida de acuerdo al derecho interno de cada Estado.

  Si hay competencia, se realizaran consultas entre los Estados involucrados para decidir qué jurisdicción es más adecuada.

El Convenio cuenta también con un apartado especial sobre Cooperación Internacional, en el cual se exponen una seria de principios que deberán regir estos procesos, asimismo, expone algunas disposiciones específicas relativas a la asistencia mutua.

Los principios son relativos a:

- **La cooperación internacional (art. 23):** Compromiso de cooperación entre los Estados partes de acuerdo a los instrumentos y acuerdos internacionales destinados para tal fin y conforme a la legislación interna de cada uno de ellos.
- **La extradición (art. 24):** Extradición entre los Estados parte de aquellos sujetos que hayan incurrido en alguno de los tipos penales señalados en este Código siempre que la pena impuesta sea mínima de un año de privación de libertad, salvo que dos o más Estados decidan la aplicación de algún tratado de extradición que disponga otro tipo de sanción en cuyo caso se aplicará la pena mínima ahí descrita. El procedimiento, condiciones y requisitos de procedencia dependerán de las disposiciones de este Convenio y del derecho interno de cada Estado.
- **La asistencia mutua (art. 25):** Compromiso de ayudo mutua para efectos de investigaciones, procedimientos o con el fin de obtención de pruebas. Salvo que se disponga lo contrario en este convenio, los procedimientos de asistencia estarán sujetos al derecho interno de cada Estado requirente o de los instrumentos internacionales adoptados por estos. Si es requerido el cumplimiento de la doble criminalidad, bastará con que exista la tipificación del delito, aunque sea en otros términos o categorías.

  En caso de no haber acuerdo internacional aplicable para la asistencia entre los Estados partes interesados, se podrá aplicar el procedimiento señalado en este Convenio (art. 27).
- **La información espontanea (art. 26):** Implique que las partes pueden comunicar información de sus propias investigaciones sobre delitos señalados en este Convenio sin previa solicitud formal.
- **Confidencialidad y restricciones de uso (art. 28):** Solo en caso de que no exista tratado entre las partes interesadas o disposiciones de derecho interno, se seguirá lo dispuesto en el presente Convenio.

En lo que respecta a la asistencia mutua, las disposiciones específicas son relativas a:

- **Medidas provisionales:**
    - Conservación rápida de datos informáticos almacenados (art. 29).
    - Revelación rápida de datos conservados (art. 30).
- **Poderes de investigación:**
    - Acceso a datos almacenados (art. 31).
    - Acceso transfronterizo a datos almacenados con consentimiento o cuando sean de acceso público (art. 32)
    - Obtención en tiempo real de datos relativos al tráfico (art. 33).
    - Intercepción de datos relativos al contenido (art. 34).

En todas estas, el Convenio establece las disposiciones que deberán aplicarse para la expedición y recibimiento de solicitudes sobre cualquiera de estos tipos de asistencia.

Finalmente, el Convenio dispone que cada Estado parte se encargará de designar un punto de contacto disponible 24/7 que permita la asistencia inmediata para investigaciones, obtención de pruebas o cualquier otro tipo de asistencia; para esto, cada Estado se encargará de garantizar la disponibilidad de personal y recursos suficientes para la adecuada funcionalidad del mismo (art.35).

En conclusión, y en palabras de Morón Lerma, el Convenio de Cibercriminalidad persigue básicamente tres objetivos en torno a los cuales se estructura, a saber:

- Armonizar el Derecho Penal material.
- Establecer medidas procesales o cautelares adaptadas al medio digital.
- Poner en funcionamiento un régimen rápido y eficaz de cooperación internacional.[128]

128. DÍAZ, Andrés. El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest. *REDUR* [En línea]. Nº. 8, 2010, pp. 196-197 [Consultado el 10 de julio de 2022]. Disponible en: https://publicaciones.unirioja.es/ojs/index.php/redur/article/view/4071/3321

4. La cooperación internacional en materia de ciberdelincuencia.

4.1. La cooperación internacional y su arquitectura.

La *Cooperación Internacional* es un conjunto de acciones y herramientas de carácter internacional orientadas a movilizar recursos e intercambiar experiencias para alcanzar metas comunes, con criterios de solidaridad, equidad, eficacia, sostenibilidad, corresponsabilidad e interés mutuo.[129]

Por tanto, la cooperación internacional se encuentra en íntima relación con el desarrollo; el *desarrollo* se refiere al proceso de cambio y crecimiento relacionado con una situación, individuo u objeto determinado. Al hablar de desarrollo podemos referirnos a diferentes aspectos: al desarrollo humano, desarrollo económico, o desarrollo sostenible.[130]

En ese sentido, es aquella que tiene como eje central el desarrollo mutuo entre los países a través de la movilización de recursos financieros, técnicos y humanos para resolver problemas específicos, fomentar el bienestar y fortalecer las capacidades nacionales.

La cooperación internacional vendría siendo entonces más que un sinónimo de simple *ayuda*, pues está dirigida a la construcción internacional de estrategias internacionales que respondan a las realidades que la globalización y el desarrollo regional y local subrayan como urgentes, en un mundo donde el respeto a las diferencias debe traducirse en políticas de Estado y acuerdos internacionales en favor de la diversidad.

129. Diccionario Prehispánico del Español Jurídico. cooperación internacional. [En línea] [Consultado el 10 de julio de 2022]. Disponible en: https://dpej.rae.es/lema/cooperaci%C3%B3n-internacional

130. Diccionario de la lengua española. Desarrollo. [En línea] [Consultado el 10 de julio de 2022]. Disponible en: https://dle.rae.es/desarrollo

La Cooperación Internacional, tiene una estructura lógica y física, de tal manera que existen tipos de cooperación, instrumentos de cooperación, modalidades de cooperación, y procesos de cooperación.

Todos estos componentes de la estructura están articulados en un determinado Sistema Nacional, en donde la cabeza estructural es la denominada Agencia Nacional de Cooperación Internacional, una Instancia Normativa a nivel de cada país que dirige las acciones de la cooperación internacional. Estas instancias sueles estar a nivel nacional, pero también a nivel regional o federal y pueden ser parte conformante de otros actores, como los mismos gobiernos regionales.

- **Fuentes de cooperación:**
    - **Cooperación oficial a través de agencias de cooperación internacional** (organismos internacionales).
    - **Cooperación no oficial a través de organismos no gubernamentales** (Fundaciones, ONG, entre otras).
- **Instrumentos de cooperación:** Formales e informales (convenios, tratados o acuerdos) (bilaterales, regionales y multilaterales).
- **Manifestación de la cooperación:**
    - **Vertical:** Cuando la cooperación es de un país desarrollado a un país subdesarrollado.
    - **Horizontal:** Cuando la cooperación se da entre países en vías de desarrollo
    - **Triangular:** Cuando un país es el vehículo de la cooperación de un país desarrollado hacia uno en vías de desarrollo.
- **Tipos de cooperación:** Cooperación técnica, financiara, científica, tecnológica, cultural, judicial, entre otras.
- **Modalidades de cooperación:** Proyectos, donaciones, asesoramiento, asistencia, capacitaciones, becas, fondos, entre otros.
- **Procesos de cooperación:** A través de políticas, investigaciones, intercambio de bienes y servicios, generación de capacidades, entre otras.

4.2. La cooperación judicial internacional en materia penal.

La Cooperación Judicial Internacional constituye toda actividad que tiene por finalidad, el coadyuvar con la justicia extranjera en su ejercicio jurisdiccional en todos sus niveles.

La Cooperación Judicial Internacional se ha convertido en la actualidad en uno de los instrumentos más eficaces y necesarios para el combate de la delincuencia organizada transnacional, así como en cualquier actividad de auxilio judicial, propiciada por el continuo y cotidiano hecho del tránsito de personas entre los Estados.

La Cooperación Judicial puede proceder en diversas materias, sin embrago, la más común ha sido la cooperación internacional judicial en materia penal, siendo esta la que nos es de interés para este estudio, pues constituye un conjunto de actos de naturaleza jurisdiccional, diplomática o administrativa que involucra a dos o más Estados y que tiene por finalidad la persecución y la solución de un hecho delictivo ocurrido en territorio cuando menos, de uno de tales Estados.

4.2.1. Algunas dificultades que afectan la cooperación internacional judicial en materia ciberdelictual.

Tras interpretar el constante desarrollo de las TICs como un fenómeno complejo cuya nueva realidad presupone una vista de la cotidianeidad desde la virtualidad, abriendo caminos anteriormente considerados inexistentes para todos, no podemos ignorar la problemática que esto a su vez representa, pues de hecho que facilita una infinidad de posibilidades para la respuesta de necesidades cotidianas, pero también, suministra igual capacidad para infringir la ley a cualquiera.

Razón por la cual, antes de satanizar su ejercicio, los gobiernos tienen la responsabilidad de definir las condiciones para que el ciberespacio y las TICs puedan emplearse a mansalva, del mismo modo que se ha hecho para garantizar

la seguridad pública y ciudadana ante el crimen tradicional o la seguridad jurídica en las relaciones entre partes.[131]

No obstante, por su singularidad con respecto a la delincuencia tradicional, este fenómeno exige de una consideración especial por parte del derecho penal, en donde la colaboración y cooperación internacional desempeñan un papel fundamental, por la ineficacia de los métodos clásicos ante:

- **La inexistencia de fronteras reales o indeterminación geográfica:** Dado el cibercrimen carece de un ente físico, encontrándose disperso en servidores por todo el mundo.
- **La facilidad de comisión:** Puesto que no requiere de excesivos recursos, ni de la presencia física del sujeto activo.
- **El problema de múltiples jurisdicciones:** Relacionado con el ámbito de aplicación espacial de la norma penal, en vista de la gran libertad que goza el ciberdelincuente para cometer delitos sin importar el territorio, ocasionado duda en todos los niveles respecto a cuál ha de ser el órgano competente y en qué lugar ha de surtir efecto la resolución.
- **La problemática de la responsabilidad penal:** *Societas delinquere non potest*, en el caso empresarial, nos encontraremos ante la problemática probatoria de las actividades ilícitas en el ciberespacio de estas, requiriendo el corroborar la actuación de ilícita de la empresa, para posteriormente identificar los distintos autores y el grado de responsabilidad de c/u.
- **El crecimiento constante y desconocido:** El expansionismo frenético de las nuevas tecnologías, cuyo desarrollo parece no tener fin, y su desconocimiento, acompañado de una escasa regulación… vuelve del sujeto pasivo un blanco muy fácil para el delincuente.

131. Ministerio Público Fiscal de la Ciudad Autónoma de Buenos Aires. Cooperación internacional en materia de seguridad. [En línea] [Consultado el 15 de julio de 2022]. Disponible en: https://sistematizacion.com.ar/cuadernillos/oea/4/4.pdf

- **Y otros problemas procesales:** crímenes que no dejan huellas, dificultad de descubrimiento y detección del delito, complejidad de recolección de evidencia etc.

Desempeñando la cooperación internacional crucial importancia para el tratamiento del cibercrimen; dependiendo para su facilitación de leyes nacionales sustantivas y procesales armonizadas, que penalicen las conductas cibercriminales y establezcan normas para la regularización de las prácticas de pruebas y procedimientos penales.

Auxiliándose además de la armonización de instrumentos bilaterales, regionales y multilaterales sobre delitos cibernéticos que permitan la cooperación, en temas de asistencia judicial recíproca y extradición, cuando exista una doble incriminación, para evitar:

- Que se creen refugios seguros para delitos cibernéticos en los que no se pueda procesar a los actores del delito.
- El desentendimiento de las obligaciones internacionales respecto al respeto de Derechos Humanos fundamentales.
- El rechazo de solicitudes de cooperación internacional por transgredir, sus resultados, obligaciones internacionales en materia de Derechos Humanos tras su respuesta.
- La producción de importantes retrasos de cooperación, tras la denegación de cooperación judicial, por la volatilidad de las pruebas digitales.
- Etc.

Quedando clara, con todo lo manifiesto, la trascendencia de la cooperación internacional para el tratamiento del cibercrimen; refiriéndose por cooperación, *in abstracta*, a la estricta relación de solidaridad intercultural que esto presupone, con la concurrencia reciproca de ideas y soluciones, ayuda mutua y nuevas formas de colaboración transversal. Siendo esta, su principal ventaja y, a la vez, un inconveniente, a causa de la complejidad y dificultad que supone articular procesos participativos entre gran cantidad de Estados, con diversas peculiaridades e intereses, para lograr acuerdos.

Dado que no se trata de un elixir universal capaz de dar respuesta a todos los problemas, sino de contribuir definitivamente a corregir muchas dificultades o al menos centrar las bases para hacerlo. Por lo que es necesario partir del rescate de prácticas diplomáticas y el esfuerzo conjunto de los Estados para dar respuesta a los problemas que les afectan.[132]

4.2.2. Algunas pautas de utilidad para una satisfactoria cooperación internacional en materia ciberdelictual:

Cualquier medida que se tome en el ámbito ciberdelictual debe tener en cuenta el carácter específico y global al que se enfrenta, y que es necesaria una visión conjunta de los problemas. La dimensión supranacional juega, por tanto, una importancia crucial en el tratamiento de los delitos informáticos; lo que hace imperativo la aplicación de procesos de cooperación internacional.

No obstante, la cooperación internacional en materia de ciberdelincuencia, como bien se estudió en el apartado que antecede, envuelve un conjunto de dificultades que generan conflicto al momento de la correspondiente prevención, persecución y sanción efectiva; lo que contribuye a la formación de lo que se podría denominar como “paraísos ciberdelictuales”, pues, una vez más, la lucha contra la ciberdelincuencia solo es posible con el auxilio y asistencia entre Estados.

Por lo tanto, dada la preeminencia de la cooperación internacional, resulta preciso preguntarse qué tipo de acciones se pueden ejecutar para hacer de este proceso un verdadero paradigma de solución ante la cibercriminalidad que permita superar aquellas dificultades que hasta el día de hoy impiden la colaboración trasversal entre los países.

A continuación, se presentarán una serie de elementos que favorecen estos procesos de cooperación, sin detrimentos de otros más que puedan incluirse:

132. DÍAZ, Andrés. Op. Cit. pp. 187-189

- **Cooperación a gran escala:**

Considerando que la cooperación internacional en materia de ciberdelincuencia requiere ser de gran alcance dadas las características propias de esta tipología de delitos (trasnacionalidad, universalidad, globalidad), resulta necesario en primera instancia que los acuerdos internacionales adoptados abarquen la mayor cantidad de Estados, por lo tanto, antes que Tratados bilaterales, es más conveniente la adopción de tratados multilaterales, pues de esa manera es posible la concreción de acciones, operaciones y estrategias a gran escala.

- **Armonización de normas sustantivas:**

La uniformidad de las normas sustantivas es otro proceso de gran relevancia para la eficacia de la cooperación internacional, dado nuevamente, al carácter trasnacional de esta tipología y la necesidad de aunar los criterios punitivos en torno a dichas conductas, pues, una puesta en común supraestatal de mismos proporciona una mayor lucidez y racionalidad a su tratamiento; pues, los sistemas contra la cibercriminalidad necesitan de coherencia y sensatez y no multiplicidad de tipos y penas con distinta aplicabilidad y entidad que origina inseguridad, asimismo, demanda evitar desigualdades por la presencia de lagunas; en otras palabras, impedir que una misma acción esté penada en un lugar y no en otro.

Actualmente, uno de los instrumentos más relevantes sobre esta materia es el Convenio de Budapest, siendo la única herramienta internacional especializada que busca la harmonización de las normas sobre cibercriminalidad.

Este Convenio se define por una verdadera plasticidad en los mandatos a los Estados, pues mantiene abiertas las posibilidades de punición, permitiendo así la aplicación flexible de los tipos, el trabajo en pos de una lucha común, el castigo de similares conductas, pero a la vez el respeto del ordenamiento jurídico propio de los Estados.

Mediante la aludida naturaleza dúctil de los tipos y la utilización de reservas, bajo expresiones del tipo «cualquier Parte podrá exigir» o «cualquier Parte podrá reservarse el derecho», el Convenio sobre Cibercriminalidad crea un sistema, no

exento de complejidad, que a *priori* garantiza la conciliación con los más diversos sistemas jurídicos.[133]

Somos conscientes de la dificultad que conlleva hacer realidad esta homogeneización, pues en efecto que el derecho penal es una parcela que ha sido reservada a la soberanía de los Estados. A pesar de esto, las ventajas que este proceso ofrece son de tal relevancia, que mientras no se lleve a cabo, la lucha contra la ciberdelincuencia se seguirá viendo obstaculizada, pues incluso si es posible cooperar a nivel internacional sin exigir la plena armonía de las legislaciones nacionales, sin esta pauta siempre habrá factores que la obstruyan.

- **Adaptación de normas procesales a las nuevas necesidades:**

Se observa que la mayoría de los problemas planteados en el apartado anterior no son constituyentes al área del derecho penal sustantivo, sino más bien al procesal: dispersión normativa, múltiples legislaciones y jurisdicciones, amplitud geográfica, responsabilidad de personas jurídicas, recolección de evidencias, vicios del proceso, demoras, ejecución de resoluciones, etc.

Al respecto, es preciso que el derecho procesal interno siga el ritmo de los avances tecnológicos, aprobando y aplicando normas relativas, por ejemplo, a las pruebas digitales, para su correspondiente admisión en investigaciones y enjuiciamientos penales, así como su compartición adecuada con asociados extranjeros encargados de hacer cumplir la ley; todo esto bajo el establecimiento de disposiciones legislativas encargadas de evaluar la autenticidad, integridad, legalidad y pertinencia de los mismos.

Asimismo, la sencilla instrumentalización de las técnicas de cooperación es otro elemento que no puede pasar desapercibido y que contribuye a facilitar procesos como el intercambio efectivo de información; componente que merece gran interés dada la universalidad del delito cibernético y la susceptibilidad de los datos a

133. DÍAZ, Andrés. Op. Cit. p. 198

cambios, ocultación o hasta eliminación. En este sentido la agilidad y rapidez serán aspectos que beneficiarán inmensamente la persecución de los delitos informáticos.

Igualmente, será muy importante para dotar de una mayor presteza a la investigación llevar a cabo una simplificación cualitativa de los medios de comunicación. A tal efecto recordamos que la utilización de Internet y las nuevas tecnologías (así como los intercambios vía Web) pueden contribuir con esta labor dotando de celeridad las gestiones de los agentes estatales.

Por otra parte, es imperativo hablar también de la extradición, materia que continúa dominada por los Tratados bilaterales y que posee tradicionalmente requisitos generalizados como la doble incriminación y especialización, reciprocidad, voluntad cooperadora y existencia de un núcleo duro insalvable constituido por los delitos políticos y la pena de muerte.

En este sentido, al menos para la materia ciberdelictual, lo ideal es que los procesos de extradición encierren límites mínimos de condena y circunstancias especiales de rechazo, planteando inclusive excepciones –en determinados casos— al principio de doble incriminación, con el objetivo de permitir el desarrollo de un proceso inevitablemente veloz, imprescindible para la adecuada persecución del delito internacional.

En otras palabras, lo recomendable para los casos relacionados con el ciberespacio, el proceso sea especializado, simplificado o abreviado; siempre bajo el respeto de los derechos humanos y fundamentales del imputado, y de la soberanía de cada Estado.

- **Colaboración entre operadores de justicia a nivel interno:**

La cooperación entre los diversos agentes nacionales; la celebración de consultas con todos los interesados correspondientes, incluidos los interesados intergubernamentales, el sector privado y la sociedad civil, las autoridades encargadas de hacer cumplir la ley, e incluso los proveedores de servicios de comunicaciones; resulta de gran interés. Estas acciones fomentarán la cooperación internacional, ya que esta se ve reforzada por la capacidad interna de los países.

- **Especialización de los operadores de justicia:**

Es menester la creación de una unidad u oficia especializada con personal altamente calificado para hacer frente a las amenazadas ciberdelictuales que se puedan generar tanto en el interior del territorio como fuera de este.

La capacidad o especialización en el tema que tratamos, juega un papel determinante, pues en nada serviría un apropiado sistema de derecho sustantivo y procesal, si los encargados de su puesta en práctica carecen de los conocimientos necesarios sobre ciberdelitos, entorpeciendo el seguimiento de los casos concretos; es por esto que los Estados deben asignar recursos suficientes para fomentar la capacidad interna a todos los niveles (jueces, fiscales, investigadores y autoridades encargadas de hacer cumplir la ley), haciendo hincapié en los problemas cada vez mayores que plantean, por ejemplo, la computación en la nube, la web oscura y otras tecnologías emergentes.

- **Recursos técnicos idóneos:**

Además de las unidades y personal especializado, se requerirán en mayor medida de equipos informáticos e instalaciones modernas, en continua actualización para que los avances tecnológicos no supongan en modo alguna ventaja a favor del delincuente.

- **Colaboración de los operadores de justicia en el plano internacional:**

Para efectos de la cooperación entre estas unidades a nivel internacional, Antonio López señala dos vías: la realizada a través de convenios internacionales y la que se sustancia mediante organizaciones internacionales ya consolidadas como INTERPOL.[134]

134. LÓPEZ, Antonio. La investigación policial en Internet: estructuras de cooperación internacional. *IDP* [En línea]. MAY-SEP 2007, Nº. 5, pp. 72-74 [Consultado el 20 de julio de 2022]. Disponible en: file:///C:/Users/Arleen/Downloads/Dialnet-LaInvestigacionPolicialEnInternetEstructurasDeCoop-2372614.pdf

En este punto merece reconocimiento la INTERPOL como la vía más efectiva para esta labor pues, en primera instancia, abarca multitud de Estados, por lo que la escala de cooperación es mayor, y además, cuenta de hecho con una red de investigadores designados que trabajan en unidades nacionales dedicadas a la delincuencia informática, a los que se denomina puntos centrales de referencia nacionales sobre delincuencia informática, a fin de facilitar el contacto operativo entre los países miembros con la máxima rapidez posible.[135]

- **Estrategias globales:**

Finalmente, cabe destacar la necesidad de planificación de estrategias a nivel global, pues con esto no sólo se optimiza la coordinación de unidades judiciales, policiales o gubernativas, sino la elaboración de políticas al más alto nivel en la prevención del delito informático.

Además de estos elementos descritos, otros de relevancia para favorecer la cooperación ante la presencia de un acuerdo internacional son:

- Disposiciones legislativas que resistan el paso del tiempo frente a futuros avances tecnológicos.
- Tipificación de conductas tecnológicamente neutral.
- Normativización terminológicamente coherente para una precisa interpretación.
- Transversalidad de los instrumentos de regulación.
- Mecanismos de negociación para la cooperación.
- Definición de limites formales y materiales de cooperación.

4.2.3. La cooperación internacional en materia de ciberdelincuencia en el contexto nicaragüense.

La ley especial de ciberdelitos, ley 1042, se refiere a la Cooperación Internacional en el Capítulo VII, Extradición (art. 43) y Asistencia Legal Mutua (art. 44).

135. DÍAZ, Andrés. Op. Cit. p. 190

La extradición consiste en la entrega que un Estado hace a otro de individuo acusado o condenado que se encuentra en su territorio para que en ese país se le enjuicie penalmente o se ejecute la pena.[136]

El referido artículo sobre extradición, como bien se explicó en el estudio del régimen nacional, remite al Código Procesal Penal a falta de Tratados o Convenios Internacionales, el cual dispone que éste puede ser de dos tipos: activa o pasiva (Art. 353-354):

- **Activa:** Se da cuando la fiscalía general de la Republica solicita ante la Sala de lo Penal de la Corte Suprema de Justicia, la extradición de una persona contra la que se hay presentado acusación y medida cautelar de privación de libertad, o cuando la misma deba descontar una pena privativa de libertad, pero se encuentra fuera del país. La Corte resolverá la procedencia de la solicitud en dentro del plazo de tres días.
- **Pasiva:** Se da cuando un gobierno extranjero solicita la extradición de una persona que se encuentra en el territorio nicaragüense. En este caso la fiscalía general de la República informará a la Sala de lo Penal de la Corte Suprema de Justicia para que resuelva. Puede darse el caso de que varios países soliciten la extradición de una misma persona, en cuyo caso de resolverá de acuerdo a lo estipulado en este código, siguiendo el trámite estipulado (art. 356 CPP). Una vez hecho esto, la Sala de lo Penal dictará resolución concediendo o negando la extradición dentro de los diez días siguientes. Contra esta resolución cabrá recurso de reposición el cual podrá ser interpuesto dentro de los tres días siguientes a partir de la notificación. Si la solicitud se deniega el reo será puesto en libertad, si es aceptada será puesto a la orden del Ministerio Publico y de la Policía Nacional para su entrega.

136. SOLÓRZANO, Karla. *La extradición en el proceso penal nicaragüense* [En línea]. Trabajo de grado para optar al título de Master en Derecho Penal y Derecho Procesal Penal. Universidad Centroamericana de Managua, 2010, p. 5 [Consultado el 20 de julio de 2022]. Disponible en: http://repositorio.uca.edu.ni/975/1/UCANI3250.pdf

Por otro lado, para la extradición por medio de Tratados y Convenios internacionales, Nicaragua a suscrito una gran cantidad de acuerdos –bilaterales en su mayoría— como, por ejemplo: El Tratado de Extradición entre Nicaragua y Costa Rica, 1893; El Tratado de Extradición de criminales entre Nicaragua y Estados Unidos, 1905; El Tratado de Extradición de criminales entre Nicaragua y España, 2000; Convención Interamericana sobre Extradición, 1981; Tratado Centroamericano relativo a la orden de detención y extradición simplificada, 2005.

Ahora bien, el artículo 43 de la referida ley, dispone también que, a falta de Convenio o Tratado Internacional, podrá prestarse o solicitarse asistencia legal mutua con base en el principio de reciprocidad establecido en el Derecho Internacional. El principio de reciprocidad es la costumbre de un Estado que concede a otro, un trato semejante al que recibe de él, con base en la cooperación internacional. [137]

El único instrumento suscrito por Nicaragua especializado en materia de ciberdelitos es el Convenio Iberoamericano de cooperación sobre investigación, aseguramiento y obtención de prueba en materia de ciberdelincuencia; no obstante, cabe mencionar que este instrumento a pesar haber sido suscrito en el 2014, no fue hasta el mes de febrero del año 2020 que fue ratificado y publicado.

Por otro lado, Nicaragua ha participado en capacitaciones a nivel internacional, por ejemplo, en la Capacitación impartida por la INTERPOL en el año 2016 sobre delitos cibernéticos en América Latina y el Caribe, la cual constó de tres sesiones en cooperación con la Policía Real de Bahamas, la Policía Nacional de República Dominicana y la Policía Nacional de Colombia.[138]

137. JARUFE, Juan. Principio de reciprocidad, y protección de derechos de migrantes y nacionales: Análisis constitucional y del Proyecto de Ley de Migración [En línea]. Chile: Biblioteca del Congreso Nacional, 2019, pp. 1-3 [Consultado el 20 de julio de 2022]. Disponible en: https://www.bcn.cl/obtienearchivo?id=repositorio/10221/27217/1/Principio_de_reciprocidad_y_proteccion_de_derechos_de_migrantes_y_nacionales._Analisis_constitucional_y_del_Proyecto_de_Ley_de_Migracion.pdf

138. INTERPOL. INTERPOL refuerza la capacidad de vigilancia del delito cibernético en América Latina y el Caribe. [En línea] [Consultado el 20 de julio de 2022]. Disponible en: https://www.interpol.int/en/News-and-Events/News/2016/INTERPOL-boosts-cybercrime-policing-capacity-in-Latin-America-and-the-Caribbean

Así mismo en el año 2021, se desarrolló el Proyecto de INTERPOL de Desarrollo de Capacidades en Ciberdelincuencia en las Américas, Fase II, que al igual que el anterior combinó actividades de evaluación, tutoría y capacitación con operaciones y esfuerzos de concientización pública para prevenir, detectar e investigar el delito cibernético de manera integral; de este proyecto Nicaragua también fue parte.[139]

A nivel interno, en el año 2020, se impartió el curso "Lucha contra los delitos en el campo de la información computarizada, a través del cual se capacitó a un total de veinte oficiales de diferentes estructuras de la Policía Nacional; este curso fue organizado por la Federación Rusa, con lo cual se evidencia una cooperación técnica entre ambos Estados con el objetivo de fortalecer las destrezas y habilidades de nuestros operadores de justicia.[140]

En el año 2021, se llevó a cabo un encuentro organizado por el Ministerio de la Juventud sobre ciberdelitos y ciberseguridad, dirigida a trabajadores de las diferentes instituciones y plataformas digitales y de comunicación; el encuentro se centró básicamente en la exposición de la ley, los tipos penales regulados, su importancia, las garantías y herramientas que ofrece.[141]

Asimismo, en el caso de la Policía Nacional, la Dirección de Investigaciones Económicas (DIE) ha creado una Unidad de Ciberdelitos para la investigación especializada de estos grupos delictivos.[142]

---

139. INTERPOL. Fortalecimiento de Capacidades en Ciberdelincuencia en las Américas. [En línea] [Consultado el 20 de julio de 2022]. Disponible en: https://www.interpol.int/en/Crimes/Cybercrime/Cyber-capabilities-development/Cybercrime-Capacity-Building-in-the-Americas

140. Policía Nacional. Oficiales concluyen con éxito capacitación en ciberdelitos. [En línea] [Consultado el 20 de julio de 2022]. Disponible en: https://www.policia.gob.ni/?p=61428

141. Tn8. Encuentro en Nicaragua para conocer de ciberdelitos y seguridad digital. [En línea] [Consultado el 20 de julio de 2022]. Disponible en: https://www.tn8.tv/nacionales/533322-encuentro-en-nicaragua-para-conocer-de-ciberdelitos-seguridad-digital/

142. SÁNCHEZ, Silvia. Perfiles del ciberdelito: un campo de estudio inexplorado. *Revista de Derecho* [En línea]. AGO-DIC 2021, No. 30, p. 74 [Consultado el 20 de julio de 2022]. Disponible en:https://www.lamjol.info/index.php/DERECHO/article/download/12223/14276/44901

4.2.3.1. Observaciones sobre la cooperación internacional en Nicaragua en materia de cibercriminalidad.

Si bien es cierto Nicaragua a suscrito una gran cantidad de Tratados y Convenios en materia de extradición, la gran mayoría de ellos son instrumentos bilaterales, por consiguiente, aún hay muchos países con los que no hay ningún tipo de acuerdo en este sentido, lo que provoca recurrir al procedimiento establecido el Código Procesal Penal.

En todo caso, los instrumentos que sí se han suscrito están bastante desactualizados, por lo que no consideran la naturaleza de los ciberdelitos, favoreciendo a que los delincuentes alteren, modifiquen, oculten o eliminen datos antes de su captura, datos que pueden resultar indispensables para su correspondiente sancionamiento.

Otro asunto que se puede mencionar es respecto a la falta de seguimiento que se la da a algunos de los instrumentos internacionales, pues a pesar de ser suscritos, no son aprobados, ejemplo de ello son los dos últimos tratados mencionados anteriormente; de los cuales el ultimo (Tratado Centroamericano relativo a la orden de detención y extradición simplificada) merece especial atención pues trata acerca de la simplificación del proceso de detención y extradición, que como se ya se mencionó, es de vital importancia para la eficaz lucha contra los ciberdelitos y para la cooperación internacional consecuentemente.

Refiriéndonos ahora a la Asistencia Legal Mutua, Nicaragua también ha suscrito diversos Convenios y Tratados Internacionales, tal como se estudió anteriormente en el apartado sobre el régimen legislativo internacional, de los cuales solo uno es dedicado a la materia especifica de ciberdelincuencia, por lo que, a pesar de que el resto puede ser usados en esta área, nuevamente no consideran la naturaleza compleja y cambiante de esta tipología de delitos contando con un enfoque bastante desfasado.

En todo caso, algunos de los problemas de estos instrumentos residen en que:

- La doble incriminación se presenta como un requisito aplicable casi en todos los casos, lo cual deja puertas para que algunos autores no sean castigados.
- Por lo general los plazos suelen ser extensos y prorrogables, por lo que hay posibilidades de que la posterior investigación y persecución resulte inefectiva.

Otra observación que puede hacerse es la no incorporación de Nicaragua al Convenio más importante sobre cibercrimen, de la actualidad, nos referimos al ya tantas veces mencionado Convenio de Budapest.

A pesar de esto, Nicaragua, como se expone en el fundamento teórico, sí toma como inspiración este instrumento al momento del establecimiento de las tipologías conductuales en la ley 1042, aunque también hace uso de otras clasificaciones como la dada por las Naciones Unidas.

En todo caso, el mayor inconveniente no se presenta tanto en la tipificación de los tipos delictivos, sino más bien, en los aspectos de tipo procedimental, pues en ese caso no se han establecido dentro del régimen legislativo nacional, ningún tipo de medida específica y determinada para, por ejemplo, la obtención en tiempo real de datos relativos al tráfico, la regulación de los medios de prueba electrónicos, entre otras cuestiones más, precisamente porque el proceso que se sigue para la investigación y persecución de los ciberdelitos en el contexto interno es el mismo destinado para los delitos tradicionales, dejándose a discreción de la autoridad judicial las medidas que se deban ordenar para la investigación u obtención y conservación de pruebas.

El Convenio Iberoamericano de cooperación sobre investigación, aseguramiento y obtención de prueba en materia de ciberdelincuencia**;** es el único de los suscritos por Nicaragua que sí considerada la naturaleza de los ciberdelitos y se enfoca en un área de gran relevancia como es el de los medios probatorios, para lo cual también ordena la designación de una autoridad que sirva como punto de contacto disponible 24/7, por lo que, debe reconocerse el esmero de Nicaragua de incluir una herramienta especializada de tal interés.

Asimismo, ha de reconocerse la labor que se ha dedicado a la participación de capacitaciones lideradas por instancias internacionales como la INTERPOL, que en efecto contribuye al reforzamiento de las capacidades de los operadores de justicia a nivel interno, y consecuentemente a los procesos de cooperación hacía otros Estados; de igual manera, los esfuerzos producidos por parte del mismo Estado de Nicaragua para estos fines.

No obstante, es importante resaltar el hecho de que, la gran mayoría de estos esfuerzos no comenzaron hasta que la ley 1042 fue expedida, por lo que, en comparación con otros países de la región, Nicaragua sigue quedándose atrás en lo que ha especialización respecta, lo que hace que dichas capacitaciones, talleres, seminarios, cursos y demás realizados hasta el momento probablemente no sean suficientes y resulte necesario de esfuerzos más intensificados y puntualizados.

Otra observación es respecto a que la mayoría de estas capacitaciones han sido bastante limitadas, es decir, enfocadas solo a ciertos sectores, principalmente gubernamentales, y dentro de ese grupo, principalmente a agentes policiales; no obstante, lo oportuno es que las capacitaciones involucren a todos los integrantes del control formal: jueces locales y de distrito de los diferentes municipios del país, fiscales, integrantes de los poderes del Estado, etc.

Por otra parte, haciendo referencia ahora a la Unidad de Ciberdelitos; de hecho, que su creación era una cuestión indispensable, tanto para la investigación y persecución de la ciberdelincuencia en el plano nacional y extraterritorial, como a efectos de la efectivad de la cooperación internacional; sin embargo, a la fecha se desconocen los datos estadísticos relacionados con la incidencia delictiva del ciberdelito en el país; lo que genera incertidumbre sobre la formación especializada del personal o el seguimiento que se le da a estos fenómenos.

5. Recapitulación.

El estudio de la regulación jurídica nicaragüense en materia de ciberdelincuencia reveló múltiples dificultades, que, a razón del tipo de investigación, se limitan a deficiencias de técnica legislativa, ambigüedades, indeterminaciones, defectuosa

gestión de las mismas para la cooperación internacional y percepción social negativa, dificultades que al ser comparadas con el régimen legislativo costarricense y salvadoreño evidenciaron que muchos de ellos no son exclusivos—sino al contrario bastante usuales—aunque si mayores en cantidad.

Si bien es cierto las problemáticas que aquí han sido identificadas se limitan a textos normativos – por lo que no se logró verificar el cumplimiento de otros elementos de eficacia que ameritan de estudios prácticos— los mismos no son más que indicadores de otras posibles complicaciones que merecen identificación y atención.

Dicho de otra manera, este estudio dio lugar a evidenciar a través de un análisis documental las múltiples deficiencias presentes en nuestro marco normativo ciberdelincuencial y en su gestión en los procesos de cooperación internacional; justificando así la necesidad que existe de un estudio especializado y completo de evaluación legislativa en base a los procesos y pautas de orientación dadas por la misma criminología que ya han sido estudiados en el segundo capítulo de este informe.

CAPÍTULO IV.

GESTIÓN DE LA POLÍTICA CRIMINAL EN NICARAGUA.

Hablar de política criminal es referirse a un conjunto de criterios que conforman un determinado sistema jurídico y que son establecidos para hacer frente a la criminalidad; y dado que la criminalidad es un fenómeno que siempre estará presente, los Estados no deben desatender esta materia, procurando antes bien la valoración de las acciones desarrolladas para prevenir y sancionar la antisocialidad.

Es por esta razón que al estudiar el control social formal no era posible omitir el análisis de la gestión político criminal en materia de ciberdelincuencia en Nicaragua, tomando como ejes de actuación los conocimientos brindados por la criminología, a fin de ofrecer críticas constructivas que contribuyan a su óptimo desarrollo.

1. Relación interactual entre la política criminal y la criminología.

La criminología al examinar sus objetos de estudio, lo hace con el propósito principal de proporcionar recomendaciones concretas que permitan prevenir y sancionar efectivamente la antisocialidad a través acciones específicas para cada caso concreto. Por su parte, la policía criminal se encarga de aplicar esos aportes de la criminología y llevarlos a la práctica.

Con todo esto, la ciencia criminológica se ocupa de recolectar datos e información acerca del fenómeno criminal con el objetivo de crear políticas criminales eficaces que luego inspiren o se expresen a través de políticas públicas o de carácter social o comunitario, y del Sistema Penal, esto es, el derecho penal material, el derecho procesal penal, el derecho penitenciario o el derecho de ejecución de penas.

2. Problemáticas actuales de la política criminal según Claus Roxin.[143]

2.1. Primera Tesis: Las penas no son de ninguna manera un medio adecuado para la lucha contra la criminalidad.

Partiendo de un conocimiento profano resulta creíble que el endurecimiento de las penas disminuye la criminalidad, sin embargo, la moderna criminología aboga, como se ha repetido en reiteradas ocasiones, en la ineficacia de las penas, principalmente aquellas privativas de libertad.

Y es que, en las sociedades, el factor delincuencial siempre estará presente, y muchos de los hechos delictivos son el resultado de situaciones como relaciones conflictivas, insoportables relaciones de pareja o entre padres e hijos, calidad de vida deplorable, crisis existenciales, miseria económica, falta de inteligencia emocional, carencia de una educación razonable, familias desavenidas, entre otras fuentes delincuenciales relacionadas en donde el sujeto encuentra en el delito la única salida.

Por lo que, en muchos de los delitos, no hay una autodeterminación criminal del autor, sino que se trata de sujetos que pudieron ser hombres de bien, pero que terminaron convirtiéndose en criminales debido a las circunstancias sociales en las que se desarrollaron (no siempre es así, pero sí a menudo); y ya cuando tales seres humanos son estigmatizados a través de los delitos, el derecho penal llega muy tarde, pues apenas es posible que encarcelando a ese hombre, se llegue a corregir su estropeada socialización.

Por ende, el grave problema de la inseguridad, la violencia y el delito, que aqueja tanto a nuestra sociedad, merece ser reflexionado no desde la posibilidad de incorporación de leyes más graves o construcción de más cárceles, sino con la intención de encontrar soluciones verdaderas con fines reparadores, lo cual es

143. ROXIN, Claus. Et al. Problemas fundamentales de política criminal y derecho penal [En línea]. México: Universidad Nacional Autónoma de México, 2002, pp. 89-99 [Consultado el 10 de junio de 2022]. Disponible en:https://www.sijufor.org/uploads/1/2/0/5/120589378/03._problemas_fundamentales_de_politica_criminal_y_derecho_.pdf

posible a través de adecuados mecanismos de prevención por medio del denominado control social informal, el cual funciona como sistema regulador primario.

Pues, el derecho penal evita la anarquía y, por tanto, es indispensable, pero se espera demasiado cuando se supone que a través de las penas se reducirá sustancialmente la criminalidad existente, cuando realmente el derecho penal debe actuar como sistema secundario y más que todo como garantía en caso de que el control informal falle.

De esta manera, existe coincidencia entre los doctrinarios en que las penas son ineficaces como método primario contra la delincuencia, o, en igual circunstancia, el agravamiento de las mismas, concluyendo que no hay evidencia suficiente que demuestre que los delitos disminuyan a mayor nivel de penalización o porque aumente la pena aplicada a los mismos.[144]

2.2. Segunda Tesis: Las penas privativas de libertad son además un medio particularmente problemático en la lucha contra la criminalidad.

El surgimiento de las penas privativas de libertad en su momento, significó un gran progreso en el sistema penal, pues con ellas relevaron otros tipos de castigos como los corporales. No obstante, con el tiempo, se han dejado ver los múltiples inconvenientes que este tipo de penas conlleva consigo, pues además de no ser las más adecuadas, resultan ser problemáticas.

Por un lado, está el problema de la resocialización. Estos procesos de resocialización han sido muy criticados debido a la falta de eficacia de los programas y estrategias establecidos para tales fines, ya sea a razón de la propia realidad de los centros penitenciarios los cuales no siempre prestan los espacios propicios, la sobrepoblación de la capacidad de los mismos, la corrupción, el limitado número de

144. Biblioteca del Congreso Nacional de Chile. Efectos del agravamiento de las penas frente a la comisión de delitos. [En línea] [Consultado el 20 de julio de 2022]. Disponible en: https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/24913/1/Efectos_del_agravamiento_de_las_penas_frente_a_la_comision_de_delitos.pdf

cupos que son ofrecidos para ser parte de ellos, la falta de recursos económicos; cuestiones que dificultan e impiden que la resocialización sea un proceso sistemático de acciones orientadas a que los internos privados de libertad puedan adquirir pautas de conducta que les permitan posteriormente reintegrarse en la sociedad.

En ese mismo sentido, es apenas posible educar a alguien hacia una vida responsable en sociedad mientras se le aparta de ella y se le ofrecen condiciones de vida tan radicalmente distintas a las de la vida en libertad, en donde el sujeto es apartado de vínculos familiares, matrimoniales y laborales.

Por lo que, en vez de ser la privación de libertad un proceso en el que se le inculcan pautas de conducta al interno para que este se convierta en un sujeto de bien en la sociedad, termina siendo un proceso con muchos efectos disociadores que dan lugar muchas veces a la marginalidad social, o aún peor, a una criminalidad mayor.

Ahora bien, la pena privativa de libertad, por si sola, y sin incluir los programas de resocialización, implican ya grandes costos económicos, incluso cuando se ejecuta en circunstancias inferiores a las humanas.

El otro problema se presenta en el momento en el que el infractor queda en libertad, pues la resocialización no es solo un proceso que deba ejecutarse dentro del sistema penitenciario, sino que, amerita de seguimientos una vez que este recupera su libertad, sin embrago, la mayoría de las veces no se lleva a cabo porque no hay recursos suficientes, por lo que el fin de la pena privativa de libertad se pierde en gran manera.

Una vez más, no se trata de eliminar las penas privativas de libertad, sino más bien de abogar por su reducción a casos exclusivamente necesarios, como los delitos más graves.

2.3. Tercera Tesis: La prevención es más efectiva que la pena.

Tal como se explicó anteriormente, la moderna criminología considera que las penas, y aún más, las privativas de libertad, resultan ineficaces para enfrentar la

criminalidad, por lo que aboga en cambio por la prevención del crimen; no pretendiendo la abolición de las penas o la acción penal, pues de hecho que ambos elementos son imprescindibles para muchos casos; se trata más bien de dirigir el foco principal al quehacer preventivo.

Pues, las grandes fuentes criminales, estudiadas anteriormente y producto de una completa ausencia de socialización familiar y de las necesidades materiales de los estratos más pobres, se pueden reducir o evitar sustancialmente mediante una buena política preventiva.

Si bien la respuesta punitiva es la panacea de los criminalistas clásicos, los legisladores y el público, según dice Ferri, el sociólogo criminalista, a partir de la observación positiva de los hechos y su génesis 'natural', juzgan como evidentemente necesarios 'otros medios de defensa'.

En esta misma línea, hace referencia a la equívoca relación entre la suavidad de las penas y la proliferación de los delitos; idea que sobreviene como uno de los rasgos salientes en el discurso 'progresista' de la actualidad a favor de la retórica de la 'mano dura' o la 'tolerancia cero'.

En contraposición, Ferri señala que un abordaje de la cuestión criminal *desde el flanco* resulta mucho más efectivo*,* pues afirma que la vida cotidiana nos enseña que para hacer “menos perniciosa la explosión de las pasiones, es preferible abordarlas de flanco, es decir, en su mismo origen, antes que atacarlas de frente”

De esta forma, el autor reconstruye una *dicotomía entre represión y prevención,* cuestionando a la primera por las siguientes razones:

- **En términos *ético-políticos,* a partir de su mirada *socialista*:** Según la sociología, la criminalidad endémica encuentra sus orígenes sociales en la desigualdad del orden burgués, aunque en la perspectiva positivista de Ferri siempre existe un resto de criminalidad natural o atávica en todo ser humano.
- **Desde argumentos *científicos,* apoyándose en el método positivo de la *sociología*:** A partir del método positivo de la sociología en el estudio del

organismo social, se muestra a la represión penal como forma de intervención que no trata con sus verdaderos orígenes.

Por estas razones, la criminología, opta por la prevención del delito antes que la sanción, deslegitimando así al derecho penal como columna vertebral y eje principal de las estrategias de acción y combate a la delincuencia, proponiendo un modelo de prevención social en el que el núcleo de las estrategias se base en la acción comunitaria y en la participación ciudadana, bajo un conjunto sistemático, cohesionado y consistente de decisiones de política gubernamental, basadas en análisis científico-sociales del fenómeno criminal, construidas con la participación del Estado y la sociedad.[145]

2.4. Cuarta tesis: El sistema de reacción penal se debe ampliar y, sobre todo, complementarlo con sanciones penales similares de carácter social constructivo.

Para el aseguramiento de una óptima prevención se requiere de un catálogo de sanciones más amplio que el actualmente implementado, con el establecimiento de penas eventuales; más allá de la pena privativa de libertad y la multa, que resulta ser muy poco.

Ha como ya se ha expresado, en las tesis anteriores, de los contras de la pena privativa de libertad, encontraremos presentes desventajas en las multas, que si bien, supone una ventaja evitativa de la pena privativa de libertad, con frecuencia demuestra también no ser un medio de sanción idóneo.

Dado que el pobre no puede pagarla y resulta injusto retenerlo por esta causa en un establecimiento penitenciario mientras que quien está solvente se puede librar con facilidad de la prisión; así mismo, es posible, que algunos logren evitar la multan

145. CHINCOYA, Héctor. ¿Política criminal, política criminológica o políticas públicas en seguridad?: Reflexiones en la coyuntura de la redacción del Plan Nacional de Desarrollo 2013-2018. *Alegatos* [En línea]. ENE-ABR 2013, No. 83, pp. 103-111 [Consultado el 22 de julio de 2022]. Disponible en: http://alegatos.azc.uam.mx/index.php/ra/article/view/279/272

al permitir que terceros la paguen o incluso al recurrir a la comisión de nuevos delitos para pagar la multa.

Lo que deja claro que la multa no es ninguna panacea y por lo tanto resulta indispensable reflexionar sobre la utilidad de otras sanciones penales; en donde podremos contemplar la posibilidad del arresto domiciliario asegurado electrónicamente y la imposición de la prohibición de conducir (incluso para delitos sin relación alguna con el tráfico de vehículos de motor), como alternativas de penas, no obstante aunque encontraremos la ventaja de que dichas penas se pueden ejecutar en el tiempo libre y llevan consigo una sensible restricción de libertad, no son apropiadas para todo el mundo.

Lo que lleva a identificar que todas las sanciones penales son objetables y precisamente por eso es necesario partir de una diferenciación subjetiva atendiendo cada caso en particular. Por lo que se propone la ampliación de sanciones penales similares, las cuales presupongan una libre participación del infractor y precisamente por eso actúen como particulares medidas sociales constructivas. Siendo estas, por ejemplo:

- En el caso requerido y contando con la enérgica disposición del infractor, el ofrecimiento de disposición de terapia;
- En delitos leves y menos graves la posibilidad de sustituir la multa o la pena privativa de libertad (hasta determinado nivel) por trabajos de utilidad pública, sea este corporal o intelectual, según la calificación del interesado, a partir de una base voluntaria, estableciendo dichas actividades, preferentemente, en tiempos laborares no habituales;
- En los casos que requieran del pago de indemnización a la víctima y exista de por medio una pena privativa de libertad que desaliente al pago de la misma, considerablemente para delitos leves y la paz jurídica, la atribución de una pena de significado sustancial que permita la compensación del autor a la víctima mediante considerables servicios o renuncias personales, y en el caso de delitos graves, considerar una suspensión condicional de la pena o su atenuación sustancial;

- En caso de perturbaciones sociales sobreseer el procedimiento penal y en su lugar imponer servicios de reparación y trabajos de utilidad pública, etc.

Cabe destacar, en lo que respecta a la posibilidad de trabajo de utilidad pública como alternativa de pena, que aunque la posición contraria es muy grande por el temor a la pérdida de puestos de trabajo, resulta ser un temor infundado, pues el Estado es pobre en casi todo el mundo; por lo que para garantizar la óptima realización de sus tareas sociales necesita de una alta fuerza de trabajo que no podrá costear con sus propios medios, siendo esta la mejor alternativa para el cumplimiento de sus tareas sociales.

Con el fin de que todo esto permita una mejor reacción estatal frente al delito, considerando las circunstancias individuales de los casos, en comparación de las que permite limitadamente la pena privativa de libertad y la multa; por lo que un amplio catálogo de sanciones resulta más eficaz en la lucha contra la delincuencia en comparación con el endurecimiento de las penas.

3. Algunos presupuestos para una adecuada política criminal.

En primera instancia, y recapitulando algunas cuestiones ya planteadas, una adecuada política criminal es aquella que:

- **Prioriza la prevención antes que la sanción, es decir, considera al derecho penal como *ultima ratio legis*:**

Una adecuada política criminal debe estar orientada y fundamentada en el cambio de las condiciones que originan un incremento en la delincuencia y no solo en actuar en respuesta a los incidentes ya ocurridos o intentando prevenirlos a través de patrullas preventivas; por lo cual debe cumplir, entre otros, con los siguientes principios:[146]

146. GARAY, Pedro. Et al. *Política criminal de represión, violencia política, formación de grupos de combate armado como asociación ilícita específica y problemas concursales* [En línea]. Memoria para optar al grado de Licenciado en Ciencias Jurídicas y Sociales. Universidad de Chile, 2007, pp. 43-56 [Consultado el 22 de julio de 2022]. Disponible en:

- **El principio de subsidiariedad:** Sólo los casos graves, en los que estén lesionados o puestos en peligro bienes jurídicos importantes cabe plantear la respuesta penal.[147]
- **Principio de la intervención mínima:** El Derecho Penal sólo puede ser usado como *última ratio legis*; de tal manera que siempre que puedan utilizarse otros medios menos drásticos para ordenar o impedir una determinada conducta con eficacia.
- **Principio de prevención:** El Estado debe orientar la política criminal hacia la prevención del delito por encima de la represión del mismo, para así optimizar los recursos para dicha labor. Este principio se relaciona con la teoría de la prevención general, que se enfoca en evitar futuras conductas ilícitas. Pero es necesario que la política criminal tenga en cuenta también la resocialización del autor del delito, por lo cual también hay relación con la prevención especial, la cual tiene como objetivo el impedir la reincidencia de hechos delictivos.

Esta labor estatal preventiva debe ejecutarse, no a través de las normas penales que utilizan las consecuencias jurídicas como motivación para la no comisión de delitos, sino a través de programas y políticas sociales. En el caso de la dimensión formal, destaca la participación de los cuerpos policiales como agentes de control formal, pues su adecuado funcionamiento y la confianza que tenga la sociedad en ella, son elementos esenciales en toda política preventiva. En la dimensión informal resalta la participación de instancias sociales y comunitarias, como iglesias, organizaciones no gubernamentales, centros educativos, etc.

En este contexto, lo ideal es que las políticas criminales involucren dentro de sus actuaciones y objetivos de prevención la participación de todas las agencias de

https://repositorio.uchile.cl/bitstream/handle/2250/113177/de-garay_r.pdf?sequence=1&isAllowed=y

147. ZÚÑIGA, Laura. Modelos de Política Criminal frente a la Criminalidad Organizada: Entre eficacia y garantías. *Revista Brasileira de Ciencias Políticas* [En línea]. JUN-ABR 2020, No. 1, p. 153 [Consultado el 22 de julio de 2022]. Disponible en: https://periodicos.pf.gov.br/index.php/RBCP/article/download/700/400/2717

control, tanto formales como informales, pues su integración es la vía más segura hacia una prevención eficaz.

- **Es respetuosa con los derechos humanos y fundamentales:**

Una política criminal que no cumple con los preceptos antes descritos suele ser por lo general una política represiva, totalitaria/autoritaria, o crítica, a través de la cual se implementan medidas restrictivas de los derechos humanos de los inculpados a fin de combatir la criminalidad y no para prevenirla y dar solución a los problemas sociales que derivan en la delincuencia habitual; disminuyéndose las garantías de los imputados; y en donde las fuerzas económicas preponderantes son el centro de atención y protección.

Un Estado que se rige bajo una política de cualquiera de estas tipologías no puede ser bajo ninguna circunstancia un Estado social de derecho, pues delega toda la labor contra la criminalidad al derecho penal, desconectándose de las demás instancias y mecanismos de control social, priorizando los intereses de ciertos grupos sociales, mientras al mismo tiempo vulnera los derechos de quienes infringen la ley.

- **Parte del mundo real considerando el fenómeno criminal y el ámbito social de aplicación:**

Una adecuada política criminal debe fundamentarse en elementos reales del fenómeno criminal, de tal manera que su estructuración tome en consideración aquellos conflictos sociales que dan nacimiento a la antisocialidad a través de objetivos claros y trasparentes, cuyos resultados puedan ser verificados por medio de mediciones constantes y concretas.

En este caso, es ideal que la política criminal se base en datos teóricos dados por la criminología, y otras ciencias conexas como la sociología, y al mismo tiempo, en estudios e investigaciones de campo, estadísticas, datos oficiales y de otros indoles, en fin, todas aquellas fuentes que reflejen el contexto criminal real de la población a quien será aplicada la política.

- **Cuenta con una arquitectura apropiadamente definida:**

Los Estados deben formular políticas criminales globales y también otras determinadas a áreas específicas; por ejemplo, en materia de violencia de género, crimen organizado; todas con sus respectivos objetivos debidamente definidos.

El problema es que la mayoría de los países no instaura de forma clara e inequívoca cuáles serán los objetivos generales y específicos de sus políticas globales y especiales, y su medida de cumplimiento a corto, mediano o largo plazo, ni los exámenes de factibilidad en los que se fundamentaron, sino que se limitan a realizar discursos ambiguos, confusos y hasta contradictorios, sobre el contenido de su política.

Todo lo anterior genera consecuentemente que no se definan adecuadamente las estrategias, planes y mecanismos por medio de las cuales se dará desempeño a las políticas, y mucho menos el impacto que su aplicación pueda generar en la realidad social.

Una de las formas, al menos en teoría, de disminuir esta problemática, puede ser la formulación de políticas criminales escritas, que incluyan todas aquellas estrategias, instrumentos y acciones formales e informales por parte del Estado y la comunidad tendientes a controlar y prevenir delitos, siempre bajo la directriz de una política criminal de derechos humanos.

A través de una política escrita es posible no solo una adecuada definición de objetivos, sino también la posibilidad de verificación de cumplimiento, evaluación y actualización.

- **Se involucra en la prevención en sus tres dimensiones:**
    - **Dimensión primaria:**

La dimensión primaria se orienta el tratamiento del fenómeno criminal desde antes de sus orígenes, atendiendo la causa del mismo mucho antes de su manifestación.

Para ello se focaliza en la atención de las carencias criminógenas, de forma que asegure el bien común, acorde a objetivos sociales de educación, socialización,

vivienda, trabajo, bienestar social y calidad de vida, como ámbito esencial para la prevención.

Y dado que la prevención primaria opera siempre a largo o mediano plazo, es posible lograr una respuesta materializada mediante estrategias de política cultural, económica y social, a fin de dotar a los ciudadanos de la capacidad social suficiente para superar de forma productiva eventuales conflictos.

Fomentando y estableciendo para ello:

- La adopción de medidas de prevención de situaciones que faciliten la delincuencia, mediante el resguardo del objeto del delito y la reducción de oportunidades delictivas;
- Fomentando el bienestar, salud, progreso y lucha contra todas las formas de privación social;
- Promoviendo valores comunitarios, responsabilidad cívica, y el respeto a los Derechos Humanos fundamentales.
- Promoviendo los procedimientos de medición social; y
- Facilitando la adaptación de los métodos de trabajo de la policía y los tribunales de justicia.

- **Dimensión secundaria:**

Como parte de la política preventiva secundaria, la sociología criminal resalta que los puntos de ataque de intervención preventiva del delito deben ser:

- Los problemas de conducta en la infancia y la adolescencia.
- El mal funcionamiento de las instituciones sociales en las 'áreas de producción del delito'.

Lo anterior a través de la noción de *desorganización social,* pues el trabajo es lidiar con las influencias sociales que afectan a los 'predelincuentes' o 'potenciales delincuentes' en las 'áreas de deterioro', intentando asegurar “el desarrollo integral de la personalidad y la buena ciudadanía”.

En este contexto, se construye la idea de una acción integral, en el sentido de la necesidad de poner en marcha una serie de diversas técnicas y procesos que

intervengan de manera 'completa' en la situación 'total' de un área de delincuencia: “un minucioso programa de planificación social”.

Se plantea entonces:

- En primer lugar, la cuestión de la integralidad, es decir, esta idea de prevención del delito como un programa social amplio y comprehensivo que bajo su dirección organice todas las 'agencias' comunitarias, por lo que se observa una segmentación territorial:
  - Definición del territorio específico por intervenir;
  - Definición de las áreas en términos de la noción de espacios de 'desorganización social' o áreas de delincuencia.
- En segundo lugar, hay un recorte que pretende identificar y enfocar el trabajo preventivo en los 'potenciales delincuentes'. Este objetivo hace eje en incorporar a estos sujetos a actividades y organizaciones que se vinculen a las necesidades, con especial referencia a las lúdicas y al tiempo libre.

En este sentido, la prevención del delito se expresa como un intento de 'organizar' lo desorganizado, es decir, organizar y programar las actividades de los destinatarios a partir de la canalización de las 'necesidades normales' para evitar las actividades patológicas, como la formación de 'pandillas', propias de la desorganización comunitaria.

- **Dimensión terciaria:**

La prevención terciaria está dirigida a grupos específicos de personas que han cometido infracciones a la ley y han ingresado al sistema penal, ya sea que cumplan con alguna pena privativa de libertad o alguna de otra índole; en todo caso la finalidad de este proceso es el mismo: intervenir para apoyar la integración social de los delincuentes.

La integración social implica en primera instancia que el delincuente desista de la delincuencia, y, por lo tanto, no reincida en la comisión de delitos.

Hay muchos factores que contribuyen al desistimiento de la delincuencia, principalmente podríamos hablar de: la motivación, capital humano (capacidades para enfrentar cambios y alcanzar metas) y capital social (trabajo, familia, relaciones personales).

Asimismo, hay otros elementos que por el contrario impiden el desistimiento de la delincuencia, como son los denominados factores de riesgo, que involucran las dificultades de aprendizaje, el abuso de sustancias, enfermedades mentales, limitaciones económicas, desafíos sociales, entre otros, los cuales deben ser tratados a través de programas especiales.

Estos programas de integración social pueden variar en dependencia de los factores que contribuyen o impiden el desistimiento y las necesidades del delincuente, de tal manera que se pueden diseñar programas para tratar con categorías específicas de delincuentes, tales como los delincuentes reincidentes, delincuentes dependientes de drogas, delincuentes juveniles, delincuentes con enfermedades mentales o delincuentes sexuales peligrosos.

De igual forma, estos programas pueden ejecutarse desde dentro de los sistemas penitenciarios (durante el cumplimiento de una pena privativa de libertad) o desde fuera (cuando la infracción no supone una pena privativa de libertad o una vez que esta ha finalizado).

En todo caso, todas las intervenciones deben ser siempre parte de un programa integral diseñado para tratar con los problemas y desafíos específicos de cada delincuente como individuo.

Desafortunadamente la mayoría de los programas de integración social, máxime aquellos que se aplican en los centros penitenciarios, suelen carecer de resultados positivos, principalmente en los países del tercer mundo a razón de la extrema pobreza, lo que implica falta de recursos técnicos y humanos; la exclusión social, la falta de acceso a atención a la salud, educación o asistencia, etc.

Por tal razón es que reafirmamos nuestra posición de que las penas privativas de libertad deben reservarse solo para los casos más graves, aplicándose al resto se

situaciones sanciones basadas en la comunidad, por ejemplo, la libertad condicional o servicio comunitario, posiblemente con algún tipo de supervisión, lo que permitiría reparar las relaciones que se vieron afectadas, evitando la marginalización y los efectos dañinos de la prisión.

Mientras que, en los casos en los que solo sea posible la aplicación de penas privativas de libertad, lo ideal es que los programas incluyan:

- Intervenciones completas basadas en la continuidad de la atención para proveer asistencia coherente a los delincuentes dentro y fuera de la prisión.
- Preparación para la reinserción desde antes que el delincuente sea liberado.
- Facilitación de la transición de la prisión hacia la comunidad.
- Reforzamiento de lo bueno logrado en las prisiones por medio de tratamiento y programas de educación.
- Continuación hasta que el éxito de la reintegración sea completo.

Con frecuencia a este enfoque se lo llama “asistencia permanente”, un modo de intervención en todo el sistema.

- **Establece lineamientos sobre el control formal:**

Las políticas criminales deben dirigirse principalmente a la prevención, pero no se pueden limitar a ella, pues es evidente que no es posible que una sociedad esté exenta de penas. Por lo tanto, la política criminal debe encargarse también de establecer las directrices sobre las que deberán regirse la producción de las normas penales, su aplicación y la ejecución de las penas.

En este mismo sentido, se considera importante que los agentes e instancias de control social formal interioricen el principio de la mínima intervención, y que las normas sean más flexibles respecto al principio de oportunidad estableciendo siempre alternativas a las penas privativas de libertad en los casos de delitos menos graves, y descriminalizando una serie de conductas contravencionales que no representen violación a bien jurídico alguno o no signifiquen un grave atentado a valores sociales, todo con el objetivo de lograr que el derecho penal se convierta

verdaderamente en *ultima ratio*, pues como ya se menciona en reiteradas ocasiones, el exceso de rigor penal no es un mecanismo eficaz en la lucha contra el fenómeno criminal, y la misma criminología señala que el delincuente no teme tanto a la pena, sino a ser descubierto, esto es, a la eficacia del sistema penal.

4. Apreciación de la realidad Político Criminal Nicaragüense en materia de ciberdelincuencia.

Antes de manifestar alguna exégesis de la realidad político criminal nicaragüense, en materia de ciberdelincuencia, resulta inexcusable identificar, antes que nada, la política criminal general de Nicaragua, para comprender las acciones tomadas frente al fenómeno criminal y la legislación que lo contempla.

Erigiéndose la Política General Integral de Nicaragua, como Política de Estado, del fortalecimiento de todo el Sistema de Justicia Penal, en lo que se requiera del Estado para la protección de los ciudadanos; bajo la prevención, persecución y sanción de los delitos, como freno a la actividad delictiva, dado el nivel de peligrosidad y gravedad de los tipos penales. Como compromiso con la seguridad de las personas y sus bienes, la paz y la justicia. [148]

Por lo que, comprendiendo la política criminal, en el marco de la realidad, como un criterio abstracto, que se relaciona especialmente con la dogmática jurídica penal, aunque no solo con esta, salvaguardando al máximo las libertades y garantías de los ciudadanos[149]; logamos identificar la Política General Integral de Nicaragua, en la actualidad, como una política teóricamente preventiva.

148. Asamblea Nacional de Nicaragua. Exposición de motivos y fundamentos código penal. [En línea] [Consultado el 24 de julio de 2022]. Disponible en: http://legislacion.asamblea.gob.ni/SILEG/Iniciativas.nsf/0/fa9710a8579f712706257dda007d962f/$FILE/Exposici%C3%B3n%20de%20Motivos%20%20y%20fundamentos%20codigo%20penal.pdf

149. BORJA, Emiliano. Sobre el concepto de la política criminal. Una aproximación a su significado desde la obra de Claus Roxin. *Revista ADPCP* [En línea]. SEP-DIC 2003, Tomo Nº. 56, Nº. 1 pp. 130-148. [Consultado el 24 de julio de 2022]. Disponible en: https://dialnet.unirioja.es/descarga/articulo/1217111.pdf

Comprendiendo dentro de su Sistema de Justicia Penal un modelo preventivo, proactivo y comunitario, característico de la fuerza de seguridad encargada de mantener el orden público y la seguridad de los ciudadanos; así mismo, se contempla un carácter más humanizado en lo que refiere a la interposición de las penas previstas por la norma penal; etc.

No obstante, el incremento de la criminalidad ha conllevado, en el sector político, a la erradica creencia de que llenando las cárceles se conseguirá contrarrestar el fenómeno criminal, contemplando el principio del Derecho penal del acto, no previsto por nuestro ordenamiento jurídico, como justificante de detención, sin tomar en consideración más aspectos que los estrictamente penales.

Como podremos apreciar en el discurso presidencial del 23 de junio de 2021, en conmemoración del 85 aniversario del natalicio del Comandante Carlos Fonseca Amador, donde el presidente Daniel Ortega manifestó que si la policía encuentra a alguien robándose una bicicleta o un celular tiene que detenerlo, aunque se trate de una persona pobre, por el incremento del temor a ser asaltado o sufrir un mayor daño por un simple teléfono; siendo este un delito, que indistintamente a sus razones sociológicas o psicológicas, debe ser procesado. Aseverando que “aquí no es cuestión, de que, porque el que tiene más, entonces a ese no lo puede tocar la fiscalía, no lo puede tocar la policía, no puede ir a los juzgados, no puede ir preso…”.[150]

Consideraciones que vuelven de la Política General Integral de Nicaragua, en su aplicación, una política represiva, dado que no existe un procedimiento definido de prevención; por lo que se espera que el sujeto cometa el delito para castigarlo, atacando al hecho y no a las causas o los factores.[151]

150. El 19 Digital. Presidente Daniel Ortega: Aquí se está juzgando a criminales que han atentado contra el país. [En línea] [Consultado el 24 de julio de 2022]. Disponible en: https://www.el19digital.com/articulos/ver/titulo:117554-presidente-daniel-ortega-aqui-se-esta-juzgando-a-criminales-que-han-atentado-contra-el-pais

151. HIKAL, Wael. La política criminal preventiva y represiva: Análisis, diferencia y propuestas desde la perspectiva criminológica. En: *El ilícito y su castigo. Reflexiones sobre la cadena perpetua, la pena de muerte y la idea de sanción en el Derecho*. Coord. CIENFUEGOS, David y

Y así, siguiendo esta línea, logramos reconocer la Política Criminal Nicaragüense, en materia de ciberdelincuencia, como una política represiva, de sanción del cibercrimen; entendiéndose por represiva a las acciones tomadas por el Estado para salvaguardar su soberanía y los derechos de los ciudadanos, limitando el empleo de las TIC bajo condiciones de seguridad, responsabilidad, libertad y confiabilidad del ciberespacio.

Incurriendo en las problemáticas comunes de las políticas basadas en el control y la represión, donde la ausencia de una respuesta integral al fenómeno criminal repercute en su efectividad, agudizando otros problemas existentes, por priorizar la respuesta punitiva y retributiva a través del sistema penal y la privación de libertad, sin considerar factores criminógenos, psicológicos y sociológicos, que permitan la implementación de medidas alternativas de justicia restaurativa.[152]

Como observamos en la Ley Nº. 1042 LEC que únicamente comprende entre sus penas la privativa de libertad, incluso en delitos menos graves y leves, y los días multas; propio de las políticas represivas de la criminalidad, lo que incide en la inefectividad de los planes y estrategias, de intereses preventivos por concentrarse principalmente la respuesta Estatal ante el fenómeno criminal en sus fuerzas de seguridad y el sistema de enjuiciamiento penal.

5. Recapitulación.

El estudio de este capítulo evidenció que los altos niveles de penalización y aumento indiscriminado de las penas, principalmente de aquellas privativas de libertad, no tienen efectos positivos significativos, sino que por el contrario, acarrean una gran cantidad de consecuencias negativas, pues los sujetos con una motivación para delinquir generalmente no consideran la penalidad futura asociada a su comportamiento delictivo, al ser considerada como un evento distante y quizás poco probable; asimismo, se preocupan, más que de la pena probable, de la mayor

CIFUENTES, Manuel. México: Editora Laguna – Fundación Académica Guerrerense, 2009, p. 160. ISBN: 978-607-7679-05-9

152. HIKAL, Wael. Op. Cit. pp. 160-174

certeza sobre la posibilidad de ser capturado; por lo que, los factores que sí ayudan a disminuir los delitos son aquellos de disuasión focalizada, relacionada con la aplicación efectiva de las penas; prevención general y especial de acuerdo a lineamientos de respeto a los derechos humanos.

Por otro lado, el estudio de la política criminal Nicaragüense, con especial énfasis en la ciberdelincuencia, ha demostrado el robustecimiento de la política penal para el tratamiento del cibercrimen, centrando su tratamiento en una política represiva y sancionadora del cibercrimen representada por la Ley No. 1042 Ley Especial de ciberdelitos, por lo que apreciamos la pena privativa de libertad como pena referente a todos los delitos previstos por la norma, alternando únicamente la pena de imposición de días multas para su tratamiento.

Análisis que, a razón del tipo de investigación, se limita a la identificación de textos normativos, mediante parámetros establecidos por la doctrina, por lo que no se logró verificar a plenitud los lineamientos empíricos que guían al poder público a la definición de su política criminal, para el tratamiento preventivo del ilícito penal, los cuales también merecen de su identificación y atención.

Por lo que, dicho de otra manera, este análisis se ha enfatizado en la concepción estricta de la política criminal, dada al examen de lo que nos marca el propio ordenamiento jurídico, el cual generalmente es empleado por los juristas y también penalistas, para el estudio de la misma, acentuándose al estudio de los férreos márgenes de la ley penal, sustantiva y adjetiva, y su repercusión en la prevención de los delitos.

DISEÑO METODOLÓGICO.

Tipo de investigación: Dogmático-Jurídica. La presente investigación pretende analizar, interpretar y aplicar el estudio de las normas jurídicas existentes en materia de ciberdelincuencia en Nicaragua desde una perspectiva abstracta, a fin de proporcionar comentarios fructíferos sobre dichas normas jurídicas, anteponiéndonos a posibles supuestos y reflexionando sobre la aplicación auxiliar de las ciencias criminológicas para el fortalecimiento del sistema de control social penal en materia de ciberdelincuencia existente en Nicaragua.

Área de investigación: Área general: Estado de derecho, gobernabilidad y democracia; y área específica: Ciencias penales y criminológicas.

Método de Investigación: La metodología a emplear, en la presente investigación, consiste en el método inductivo-deductivo, dado que se pretende partir del estudio de lo particular a lo general, a fin de garantizar su correcta síntesis, mediante observancias válidas. Así mismo, se pretende hacer uso del método de Derecho comparado, a fin de actualizar el material bibliográfico actualmente disponible en nuestra alma máter y revelar los modelos más éxitos de los países estudiados.

Enfoque de Investigación: El enfoque de esta investigación es cualitativo a través del cual se pretende analizar, interpretar, describir y comprender nuestro objeto de estudio, esto es, el control social penal en materia de ciberdelincuencia en Nicaragua a través de la criminología, con el objetivo de brindar juicios que de alguna manera permitan su fortalecimiento.

Técnica de Investigación: La técnica utilizada en esta investigación será la recolección de datos por medio de la revisión documental.

Instrumentos de Investigación: Los instrumentos utilizados serán todas aquellas fuentes documentales en materia de criminología, control social penal, políticas criminales y ciberdelincuencia, tales como: Leyes, convenios, enciclopedias jurídicas, artículos jurídicos, revistas jurídicas, fichas documentales, libros, sitios web, entre otras.

CONCLUSIONES GENERALES.

Tras el análisis elaborado para este informe final y teniendo como eje central el dar respuesta a nuestras preguntas de investigación a través de los objetivos planteados, se ha llegado a las siguientes consideraciones conclusivas:

- La criminología como ciencia especializada en el estudio del fenómeno criminal nos proporciona una serie de pautas metodológicas de gran utilidad para el procedimiento de evaluación legislativa, las cuales prometen un mayor nivel de asertividad en los resultados perseguidos. Estas pautas se refieren a la importancia de la recolección de información provenientes de diversas fuentes, la necedad de sinterización de la información recolectada en datos estadísticos, así como de enfoques debidamente delimitados de valoración normativa. Con la aplicación de estos parámetros criminógenos es posible que el procedimiento de evaluación revele certeramente el impacto y funcionalidad de las normas, siempre y cuando, claro está, este sea llevado a cabo bajo la arquitectura de un idóneo proceso de evaluación tal como se expuso en el desarrollo del capítulo II de este informe; esto es, bajo una autoridad, un procedimiento, un periodo, mecanismos, instrumentos, técnicas y objetivos y fines debidamente definidos.

- El marco legislativo nicaragüense en materia de ciberdelincuencia se ve revestido de una serie de dificultades que impiden su correspondiente eficacia instrumental. La principal deficiencia que pudo ser evidenciada es la falta de aplicación de una depurada técnica legislativa, lo que se traduce en ambigüedades e indeterminaciones, asimismo resalta la no previsión de elementos que consideran la naturaleza compleja y cambiante de los ciberdelitos, además de la percepción negativa de la norma fundamentada primordialmente en su ilegitimidad. Por otro lado, en el plano internacional, Nicaragua posee una arquitectura bastante débil contra la ciberdelincuencia, careciendo de capacitaciones integrales y de gran alcance para los operadores de justicia referentes a la prevención y persecución de los ciberdelitos dentro y fuera del territorio nacional; contando asimismo en su mayoría solo con

convenios de asistencias legal mutua, que como ya se predicó, no son suficientes para hacer frente a la cibercriminalidad pues es necesario no solo del auxilio entre Estados, sino de una verdadera cooperación internacional. Todo esto solo refuerza la necesidad que existe de una evaluación legislativa completa y especializada para averiguar qué otros elementos son o no atendidos con el fin de proponer mejoras y reformas relevantes y realistas.

- En el análisis de la Política Criminal Nicaragüense en materia de ciberdelincuencia apreciamos la necesaria relación de factores Criminógenos, Psicológicos y Sociológicos con la Dogmática Penal para el eficiente establecimiento de una política criminal que permita, a raíz de la crítica del derecho vigente, la creación de propuestas que orienten eficientemente el control de los comportamientos desviados mediante la prevención. Preferentemente mediante una política criminal escrita que facilite el análisis de su aplicación, en función de los criterios marcados en los momentos anteriores, sin que esta pueda distorsionarse o parcializarse en su aplicación.

RECOMENDACIONES.

- Realizar una evaluación legislativa sobre la ley 1042, Ley Especial De Ciberdelitos a fin de identificar los factores que obstaculizan su eficacia instrumental y plantear así recomendaciones que permitan la debida subsanación de los mismos. Para estos efectos se ha propuesto la aplicación del proceso *ex post* en conjunto con las pautas metodológicas expuestas y fundamentadas en la criminología.
- Procurar que los operadores de justicia encargados de la investigación y persecución de los ciberdelitos sean altamente especializados en la materia ciberdelictual y criminológica, cuya capacitación y aprendizaje sea continuo a fin de seguir el ritmo de las nuevas tecnologías y la influencia de estas en la cibercriminalidad.
- Realizar labores de concientización sobre los riesgos que implica el uso inadecuado de las tecnologías de la información y la comunicación y los sistemas informáticos, y la necesidad consecuente de mecanismos de ciberseguridad.
- Proporcionar recursos económicos para la adquisición de instrumentos de alto rendimiento y de la más alta tecnología que permitan eficazmente la investigación y persecución de ciberdelitos cometidos dentro y fuera del territorio nacional, así como la cooperación efectiva con otros Estados, impidiendo que los avecen tecnológicos representen una ventaja a favor del ciberdelincuente.
- Fomentar el dialogo activo y la colaboración entre todos los operadores de justicia a nivel nacional, así como la colaboración entre estos y los proveedores de servicios de comunicaciones a fin de facilitar los procesos de investigación y persecución de los ciberdelitos.
- Promulgar políticas criminales basadas en una comprensión amplia del concepto general de ciberseguridad, no solo abarcando la conducta ilícita, sino —y principalmente— la disuasión delictiva, la prevención general y especial del delito, y la prestación de asistencia a las víctimas y a la población en general; para lo cual deberá estar fundamentada en el saber criminológico, el respeto a

los derechos humanos y la deslegitimación del derecho penal como columna vertebral contra la criminalidad.

- Gestionar la formulación de una política criminal escrita en materia que cibercriminalidad que facilite el análisis y verificación de su aplicación en función de los criterios y objetivos definidos.
- Procurar la adopción de convenios y tratados multilaterales sobre cibercriminalidad que faciliten los procesos de cooperación internacional a una escala mayor.
- Actualizar el sitio web oficial de la Policía Nacional dedicada a la realización de trámites en línea, incorporando las tipologías delictivas reguladas en la Ley de Ciberdelitos a fin de que los individuos de la sociedad puedan denunciar cualquier ciberataque del que sean víctimas de forma fácil y rápida.

FUENTES DE LA INFORMACIÓN.

Tratados internacionales:

- Convención Interamericana sobre Asistencia Mutua en Materia Penal, hecha en Bahamas, el día 23 de mayo de 1992. Aprobado y ratificado por Nicaragua, a través del DECRETO PRESIDENCIAL No. 77-2002 del 29 de agosto de 2002, publicado en La Gaceta – Diario Oficial, No. 173, del 12 de septiembre del 2002.
- Convenio de las Naciones Unidas contra la Delincuencia Organizada Transnacional, hecho en Italia, el día 14 de diciembre del 2000. Aprobado por Nicaragua, a través del DECRETO A.N. No. 3246 del 13 de febrero de 2002, publicado en La Gaceta – Diario Oficial, No. 38, del 25 de febrero de 2002 y ratificado mediante DECRETO PRESIDENCIAL No. 62-2002 del 18 de junio de 2002, publicado en La Gaceta – Diario Oficial, No. 121 del 28 de junio de 2002.
- Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de prueba en materia de Ciberdelincuencia, hecho en Madrid, el día 28 de mayo de 2014. Aprobado por Nicaragua, a través del DECRETO A.N. No. 8651 del 25 de febrero de 2020, publicado en La Gaceta – Diario Oficial, No. 42, del 03 de marzo de 2020 y ratificado mediante DECRETO PRESIDENCIAL No. 08-2020 del 16 de abril de 2020, publicado en La Gaceta – Diario Oficial, No. 73 del 24 de abril de 2020.
- Convenio sobre la ciberdelincuencia, hecho en Budapest, el día 23 de noviembre de 2001.
- Tratado de asistencia legal mutua en asuntos penales entre las repúblicas de El Salvador, Guatemala, Honduras, Nicaragua, Costa Rica y Panamá, hecho en Guatemala, el día 29 de octubre de 1993. Aprobado por Nicaragua, a través del DECRETO A.N. No. 1902 del 11 de junio de 1998, publicado en La Gaceta – Diario Oficial, No. 116, del 23 de junio de 1998 y ratificado mediante DECRETO PRESIDENCIAL No. 40-99 del 24 de marzo de 1999, publicado en La Gaceta – Diario Oficial, No. 68 del 14 de abril de 1999.

Leyes Nacionales:

Nicaragua:

- Constitución Política de la República de Nicaragua con reformas incorporadas. La Gaceta - Diario Oficial, del 18 de febrero de 2014, No. 32. Disponible en: https://www.asamblea.gob.ni/assets/constitucion.pdf
- Decreto ejecutivo No. 36-2012, “reglamento de la ley No. 787”. La Gaceta - Diario Oficial, del 19 de octubre de 2012, No. 200. Disponible en: http://legislacion.asamblea.gob.ni/normaweb.nsf/($All)/7BF684022FC4A2B406257AB70059D10F?OpenDocument
- Ley No. 1042, “Ley Especial de Ciberdelitos”. La Gaceta – Diario Oficial, del 30 de octubre de 2020, No. 201. Disponible en: http://legislacion.asamblea.gob.ni/normaweb.nsf/($All)/803E7C7FBCF44D7706258611007C6D87
- Ley No. 406, “Código Procesal Penal de Nicaragua”. La Gaceta - Diario Oficial, del 21 y 24 de diciembre del 2001, Nos. 243 y 244. Disponible en: https://www.poderjudicial.gob.ni/pjupload/spenal/pdf/2001_ley02.pdf
- Ley No. 621, “ley de acceso a la información pública”. La Gaceta - Diario Oficial, del 22 de junio de 2007, No. 118. Disponible en: http://legislacion.asamblea.gob.ni/Normaweb.nsf/($All)/675A94FF2EBFEE9106257331007476F2
- Ley No. 641, “Código Penal de la República de Nicaragua”. La Gaceta - Diario Oficial, del 5, 6, 7, 8 y 9 de mayo de 2008, No. 83, 84, 85, 86 y 87. Disponible en: http://legislacion.asamblea.gob.ni/normaweb.nsf/9e314815a08d4a6206257265005d21f9/1f5b59264a8f00f906257540005ef77e?OpenDocument
- Ley No. 787, “ley de protección de datos personales”. La Gaceta - Diario Oficial, del 29 de marzo de 2012, No. 61. Disponible en: http://legislacion.asamblea.gob.ni/normaweb.nsf/9e314815a08d4a6206257265005d21f9/e5d37e9b4827fc06062579ed0076ce1d

- Ley No. 983, “Ley de justicia constitucional”. La Gaceta – Diario Oficial, del 20 de diciembre de 2018, No. 247. Disponible en: http://legislacion.asamblea.gob.ni/normaweb.nsf/9e314815a08d4a6206257265005d21f9/1323c5d29a709b9c0625837c005a2b21?OpenDocument

Costa Rica:

- Constitución Política de la República de Costa Rica con reformas incorporadas. Colección de leyes y decretos, año 1949, semestre 2, tomo 2, p. 724. Disponible en: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=871&nValor3=0&strTipM=TC
- Ley No. 4573, “Código Penal”. La Gaceta - Diario Oficial, del 15 de noviembre de 1970, Alcance 120ª, No. 257. Disponible en: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=5027&nValor3=0&strTipM=TC
- Ley No. 7594, “Código Procesal Penal”. La Gaceta – Diario Oficial, del 04 de junio de 1996, Alcance 31, No. 106. Disponible en: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=41297&nValor3=0&strTipM=TC
- Ley No. 8968, “Ley de Protección de la Persona frente al tratamiento de sus datos personales”. La Gaceta – Diario Oficial, del 05 de septiembre de 2011, No. 170. Disponible en: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=70975&nValor3=85989&strTipM=TC
- Ley No. 9048, “Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal”. La Gaceta – Diario Oficial, del 06 de noviembre de 2012, Alcance 172, No. 214. Disponible en: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=73583&nValor3=90354&strTipM=TC

El Salvador:

- Decreto No. 1030, “Código Penal”. Actualizado hasta las reformas del Decreto No. 374. La Gaceta – Diario Oficial, del 14 de junio de 2022, Tomo No. 435, No. 112. Disponible en: https://www.jurisprudencia.gob.sv/busqueda/showFile.php?bd=2&data=DocumentosBoveda%2FD%2F2%2F1990-1999%2F1997%2F06%2F886E3.PDF&number=558819&fecha=10/06/1997&numero=CODIGO=PENAL&cesta=0&singlePage=false%27
- Decreto No. 108, “Ley especial contra actos de terrorismo”. Actualizada hasta las reformas del Decreto No. 341. La Gaceta – Diario Oficial, del 30 de marzo de 2022, Tomo No. 434, No. 65. Disponible en: https://www.jurisprudencia.gob.sv/busqueda/showFile.php?bd=2&data=DocumentosBoveda%2FD%2F2%2F2000-2009%2F2006%2F10%2F889E6.PDF&number=559590&fecha=17/10/2006&numero=LEY=ESPECIAL=CONTRA=ACTOS=DE=TERRORISMO&cesta=0&singlePage=false%27
- Decreto No. 260, “Ley especial contra los delitos informáticos y conexos”. Actualizada hasta las reformas del Decreto No. 236. La Gaceta – Diario Oficial, del 12 de enero de 2022, Tomo No. 434, No. 8. Disponible en: https://www.jurisprudencia.gob.sv/DocumentosBoveda/D/2/2010-2019/2016/02/B6B74.PDF
- Decreto No. 38, “Constitución Política de la Republica de El Salvador”. Actualizada hasta las reformas del Decreto N.º. 707. La Gaceta – Diario Oficial, del 19 de junio de 2014, Tomo N.º. 403, No. 112. Disponible en: https://www.asamblea.gob.sv/sites/default/files/documents/decretos/171117_072857074_archivo_documento_legislativo.pdf
- Decreto No. 551, “Ley especial para sancionar infracciones aduaneras”. Actualizada hasta las reformas del Decreto No. 18. La Gaceta – Diario Oficial, del 05 de junio de 2018, Tomo No. 419, No. 102. Disponible en:

https://www.jurisprudencia.gob.sv/DocumentosBoveda%2FD%2F2%2F2000-2009%2F2001%2F10%2F889FF.PDF

- Decreto No. 733, “Código Procesal Penal”. Actualizado hasta las reformas del Decreto No. 339. La Gaceta – Diario Oficial, del 30 de marzo de 2022, Tomo No. 434, No. 65. Disponible en: https://www.jurisprudencia.gob.sv/busqueda/showFile.php?bd=2&data=DocumentosBoveda%2FD%2F2%2F2000-2009%2F2009%2F01%2F89AA7.PDF&number=563879&fecha=30/01/2009&numero=CODIGO=PROCESAL=PENAL&cesta=0&singlePage=false%27

Doctrina:

- Administración General del Estado. Procedimiento Administrativo Común Régimen Jurídico del Sector Público [En línea]. España: Editorial BOE, 2022, pp. 408. ISBN: 978-84-340-2259-1 [Consultado el 20 de julio de 2022]. Disponible en: https://www.boe.es/biblioteca_juridica/abrir_pdf.php?id=PUB-PB-2022-140
- GONZÁLEZ, Marta. El control social desde la criminología [En línea]. Cuba: Editorial Feijóo, 2010, pp. 135. ISBN: 978-959-250-582-7 [Consultado el 03 de marzo de 2022]. Disponible en: https://dspace.uclv.edu.cu/bitstream/handle/123456789/12302/Control_Social-1.pdf?sequence=1&isAllowed=y
- HIKAL, Wael. Introducción al estudio de la Criminología [En línea]. México: Editorial Porrúa, SA, 2013, p. 252. ISBN: 978-607-09-1475-1 [Consultado el 03 de marzo de 2022]. Disponible en: https://www.scenacriminis.com/wp-content/uploads/2017/09/Introduccion-al-Estudio-de-la-Criminologia.pdf
- HIKAL, Wael. La política criminal preventiva y represiva: Análisis, diferencia y propuestas desde la perspectiva criminológica. En: El ilícito y su castigo. Reflexiones sobre la cadena perpetua, la pena de muerte y la idea de sanción en el Derecho. Coord. CIENFUEGOS, David y CIFUENTES, Manuel. México: Editora Laguna – Fundación Académica Guerrerense, 2009, p. 160. ISBN: 978-607-7679-05-9

- MIRÓ, Fernando. El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio [En línea]. Madrid: Marcial Pons, 2012. pp. 332. [Consultado el 11 de abril de 2022]. Disponible en: https://www.marcialpons.es/media/pdf/9788415664185.pdf
- OCDE. La Evaluación de Leyes y Regulaciones: El Caso de la Cámara de Diputados de Chile [En línea]. París: OCDE, 2012, pp. 103. ISBN: 978-92-64-17636-2 [Consultado el 24 de julio de 2022]. Disponible en: https://read.oecd-ilibrary.org/governance/la-evaluacion-de-leyes-y-regulaciones_9789264176362-es
- OLIVEIRA, Edmundo. "Globalización, red cibernética y delito por internet". En: "Justicia penal, política criminal y Estado social de derecho en el siglo XXI". Coord. TIFFER, Carlos. Argentina: EDIAR, 2015, p. 677. ISBN: 978-950-574-329-2
- PALIERO, Carlo. "Problemas y perspectivas de la responsabilidad penal de la persona jurídica en el derecho penal italiano". En: "Responsabilidad penal de las personas jurídicas". Coord. HURTADO, José. España: Grijley, 1997, pp. 47-74. [En línea] [Consultado el 20 de julio de 2022]. Disponible en: https://perso.unifr.ch/derechopenal/assets/files/anuario/an_1996_05.pdf
- PÉREZ, Héctor. Manual de Técnica Legislativa. [En línea] Buenos Aires: Konrad Adenauer Stiftung, 2007, pp. 219. ISBN 978-987-1285-07-5 [Consultado el 20 de julio de 2022]. Disponible en: https://www.kas.de/c/document_library/get_file?uuid=591625b8-e7d7-77d2-f52b-a340e36d83ae&groupId=287460

Otros Documentos:

- AGUIRRE, Eduardo. Control Social [En línea]. Seminario sobre aportaciones teóricas y técnicas recientes. Universidad Nacional de la Pampa, 2008, pp.61. [Consultado el 03 de marzo de 2022]. Disponible en: http://www.biblioteca.unlpam.edu.ar/rdata/tesis/e_puecon623.pdf
- ALVAREZ, Germán; MONTENEGRO, María y MARTÍNEZ, José. "Notas para la historia de la criminología". [En línea]. México: Facultad de Psicología, UNAM,

2012, pp. 23. [Consultado el 15 de abril de 2022]. Disponible en: http://www.psicologia.unam.mx/documentos/pdf/publicaciones/Notas_para_la_Historia_de_la_Criminologia_Alvarez_Diaz_Montenegro_Nunez_Martinez_Manuel_TAD_7_8_y_9_sem.pdf

- Asamblea Nacional de Nicaragua. Exposición de motivos y fundamentos código penal. [En línea] [Consultado el 24 de julio de 2022]. Disponible en: http://legislacion.asamblea.gob.ni/SILEG/Iniciativas.nsf/0/fa9710a8579f712706257dda007d962f/$FILE/Exposici%C3%B3n%20de%20Motivos%20%20y%20fundamentos%20codigo%20penal.pdf
- CASADO, José. Et al. Código Procesal Penal de El Salvador Comentado - Tomo I [En línea]. San Salvador: Consejo Nacional de Judicatura, 2004, pp. 968. [Consultado el 10 de julio de 2022]. Disponible en: https://www.cnj.gob.sv/images/documentos/pdf/ecj/publicaciones/codigoprocesalpenal_tomoi.pdf
- GARCÍA-PABLOS, A. La Aportación de la Criminología [En línea]. Cuaderno del Instituto Vasco de criminología, San Sebastián No. 3, 1989, pp. 79-94. [Consultado el 06 de abril de 2022]. Disponible en: https://www.ehu.eus/documents/1736829/2163271/09+-+La+aportacion+de+la+criminologia.pdf
- JARUFE, Juan. Principio de reciprocidad, y protección de derechos de migrantes y nacionales: Análisis constitucional y del Proyecto de Ley de Migración [En línea]. Chile: Biblioteca del Congreso Nacional, 2019, pp. 7. [Consultado el 20 de julio de 2022]. Disponible en: https://www.bcn.cl/obtienearchivo?id=repositorio/10221/27217/1/Principio_de_reciprocidad_y_proteccion_de_derechos_de_migrantes_y_nacionales._Analisis_constitucional_y_del_Proyecto_de_Ley_de_Migracion.pdf
- OSSORIO, Manuel. Diccionario de Ciencias Jurídicas, Políticas y Sociales [En línea]. Guatemala: Datascan, S.A, 2018 [Consultado el 11 de marzo de 2022]. Disponible en: https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpb

nxjb25zdWx0b3Jlc2xlZ2FsZXNkZWxub3Jlc3RlfGd4OjVjMTM0NzQ5MWYyMmIyMDE

- QUEZADA, Martha. Análisis jurídico de la ley 1042: “Ley especial de ciberdelitos” [En línea]. Nicaragua: Poder Judicial, 2021, pp. 39. [Consultado el 10 de junio de 2022]. Disponible en: https://www.poderjudicial.gob.ni/iaej/pdf/Reformas/ANALISIS%20JURIDICO%20LEY%201042.%20LEY%20ESPECIAL%20DE%20CIBERDELITOS.pdf
- ROXIN, Claus. Et al. Problemas fundamentales de política criminal y derecho penal [En línea]. México: Universidad Nacional Autónoma de México, 2002, pp. 89-99 [Consultado el 10 de junio de 2022]. Disponible en: https://www.sijufor.org/uploads/1/2/0/5/120589378/03.-_problemas_fundamentales_de_politica_criminal_y_derecho_.pdf
- TAMARIT, Josep. La política criminal como disciplina empírica y valorativa [En línea]. España: UOC, 2016, pp. 16. [Consultado el 04 de junio de 2021]. Disponible en: https://openaccess.uoc.edu/webapps/o2/bitstream/10609/92529/1/Pol%c3%adtica%20criminal_M%c3%b3dulo%202_%20La%20pol%c3%adtica%20criminal%20como%20disciplina%20emp%c3%adrica%20y%20valorativa.pdf
- UNODC. Convención de las Naciones Unidas contra la delincuencia organizada transnacional y sus protocolos [En línea]. Nueva York: Naciones Unidas, 2004, pp. 85. [Consultado el 10 de junio de 2022]. Disponible en: https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-s.pdf

Trabajos y Tesis:

- FONSECA, Xóchitl y FONSECA, Rosalba. Política Criminal y Sistema Penitenciario Nicaragüense [En línea]. Tesis de titulación de licenciatura en Derecho. UNAN-León, 2007, pp. 137. [Consultado el 03 de marzo de 2022]. Disponible en: http://riul.unanleon.edu.ni:8080/jspui/retrieve/3034
- FUENTES, María, et al. Análisis de la política criminal en el salvador [En línea]. Tesis de titulación de licenciatura en Ciencias Jurídicas. Universidad de El

Salvador, 2005, pp. 169 [Consultado el 03 de marzo de 2022]. Disponible en: https://ri.ues.edu.sv/id/eprint/7551/1/ANALISIS%20DE%20LA%20POLITICA%20CRIMINAL%20EN%20EL%20SALVADOR.pdf

- GARAY, Pedro. Et al. Política criminal de represión, violencia política, formación de grupos de combate armado como asociación ilícita específica y problemas concursales [En línea]. Memoria para optar al grado de Licenciado en Ciencias Jurídicas y Sociales. Universidad de Chile, 2007, pp. 403. [Consultado el 22 de julio de 2022]. Disponible en: https://repositorio.uchile.cl/bitstream/handle/2250/113177/de-garay_r.pdf?sequence=1&isAllowed=y
- MAÑAS, Vanessa. Responsabilidad penal corporativa y cibercriminalidad. El compliance penal relativo al Derecho de las TIC [En línea]. Trabajo de grado. Universidad de Barcelona, 2017, pp. 134. [Consultado el 24 de julio de 2022]. Disponible en: http://diposit.ub.edu/dspace/bitstream/2445/119488/1/TFG%20%20Vanessa%20Ma%C3%B1as.pdf
- MOREIRA, Darwin. Evolución de la Política Criminal [En línea]. Tesis de titulación en Jurisprudencia y Título de Abogado. Universidad Nacional de Loja. Ecuador, 2016, pp. 63. [Consultado el 03 de marzo de 2022]. Disponible en: https://dspace.unl.edu.ec/jspui/bitstream/123456789/16904/1/Darwin%20Daniel%20Moreira%20Celi.pdf
- OSORIO, Valentina y CORREA, Laura. La eficacia en el ordenamiento jurídico colombiano: El caso de la ley 789 de 2002 [En línea]. Trabajo de grado. Universidad EAFIT de Medellín, 2010, pp. 114. [Consultado el 24 de abril de 2022]. Disponible en: https://repository.eafit.edu.co/bitstream/handle/10784/12065/Valentina_CoulsonOsorio_Laura_Ram%C3%ADrezCorrea2010.pdf?sequence=2&isAllowed=y
- PASCUAL, Ivan. Ciberdelincuencia. Desarrollo y persecución tecnológica [En línea]. Tesis de titulación en Telemática. Universidad Politécnica de Madrid, 2013, pp. 159. [Consultado el 03 de marzo de 2022]. Disponible en: https://www.google.com/search?q=PASCUAL%2C+Ivan.+Ciberdelincuencia.+D

esarrollo+y+persecuci%C3%B3n+tecnol%C3%B3gica&oq=PASCUAL%2C+Ivan.+Ciberdelincuencia.+Desarrollo+y+persecuci%C3%B3n+tecnol%C3%B3gica&aqs=chrome.69i57.4427820j0j7&sourceid=chrome&ie=UTF-8#

- SOLÓRZANO, Karla. La extradición en el proceso penal nicaragüense [En línea]. Trabajo de grado para optar al título de Master en Derecho Penal y Derecho Procesal Penal. Universidad Centroamericana de Managua, 2010, pp. 73. [Consultado el 20 de julio de 2022]. Disponible en: http://repositorio.uca.edu.ni/975/1/UCANI3250.pdf

Revistas:

- ARROYO, Sergio. Estudios criminológicos contemporáneos (IX): La Cibercriminología y el perfil del ciberdelincuente. Revista de Derecho y Cambio Social [En línea]. ABR-JUN 2020, No. 60, pp. 470-512. [Consultado el 04 de marzo de 2022]. Disponible en: file:///C:/Users/cash%20america/Downloads/DialnetLaCibercriminologiaYElPerfilDelCiberdelincuente-7524987.pdf
- BORJA, Emiliano. Sobre el concepto de la política criminal. Una aproximación a su significado desde la obra de Claus Roxin. Revista ADPCP [En línea]. SEP-DIC 2003, Tomo No. 56, No. 1 pp. 113-150. [Consultado el 24 de julio de 2022]. Disponible en: https://dialnet.unirioja.es/descarga/articulo/1217111.pdf
- CAVERO, Pedro. La criminología y la ineficiencia del control social frente a la realidad peruana. Revista electrónica del Centro de estudios de Criminología de la USMP [En línea]. No. 3, pp. 1-12. [Consultado el 17 de marzo de 2022]. Disponible en: https://www.usmp.edu.pe/derecho/centro_inv_criminologica/revista/articulos_revista/2013/Criminologia_Ineficiencia_Control_Social.pdf
- CHAPMAN, Willian. El concepto de sociabilidad como referente del análisis histórico. Investigación & Desarrollo [En línea]. ENE-JUN 2015, No. 1, pp. 1-37. [Consultado el 24 de abril de 2022]. Disponible en: https://www.redalyc.org/pdf/268/26839041001.pdf

- CHINCOYA, Héctor. ¿Política criminal, política criminológica o políticas públicas en seguridad?: Reflexiones en la coyuntura de la redacción del Plan Nacional de Desarrollo 2013-2018. Alegatos [En línea]. ENE-ABR 2013, No. 83, pp. 99-116. [Consultado el 22 de julio de 2022]. Disponible en: http://alegatos.azc.uam.mx/index.php/ra/article/view/279/272
- DÍAZ, Andrés. El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest. REDUR [En línea]. 2010, No. 8, pp. 169-203. [Consultado el 10 de julio de 2022]. Disponible en: https://publicaciones.unirioja.es/ojs/index.php/redur/article/view/4071/3321
- JÄÄSKELÄINEN, Federico. La evaluación ex post de las normas: un análisis del nuevo modelo español. ASAMBLEA, revista parlamentaria de la Asamblea de Madrid [En línea] No. 36, 2017, pp. 139-176. [Consultado el 28 de mayo de 2022]. Disponible en: https://www.asambleamadrid.es/documents/20126/64823/R.36._Federico_de_Montalvo_Jaaskelainen.pdf/c1474fd5-ffde-8876-8c12-20b621e73a6d
- LÓPEZ, Antonio. La investigación policial en Internet: estructuras de cooperación internacional. IDP [En línea]. MAY-SEP 2007, No. 5, pp. 63-74. [Consultado el 20 de julio de 2022]. Disponible en: https://dialnet.unirioja.es/descarga/articulo/2372614.pdf
- LÓPEZ, Luis. Sistema y Control Social: Enfoque general. Revista SAPERE [En línea]. ENE-MAY 2015, No. 8, pp. 1-7. [Consultado el 01 de marzo de 2022]. Disponible en: https://derecho.usmp.edu.pe/instituto/revista/articulos/2012/Control_Social.pdf
- MORALES, Emma. Algunas reflexiones sobre política criminal y sus principales tendencias. Revista Nuevo Derecho [En línea]. Enero-junio de 2010, No. 6, pp. 19-28. [Consultado: 04 de marzo de 2021]. Disponible en: file:///C:/Users/cash%20america/Downloads/Dialnet-AlgunasReflexionesSobrePoliticaCriminalYSusPrincip-5549131.pdf
- RISOTO, Lucas. Una Aproximación al estudio de lo imaginario en la ilustración: El caso de Franz Antón Mesmer. Revista de Filosofía [En línea]. No. 1 2012, pp.

74-83. [Consultado el 06 de abril de 2022]. Disponible en: https://dialnet.unirioja.es/descarga/articulo/6297605.pdf

- RUBIO, Mauricio. Evaluación de las leyes: Lecciones de la criminología. Revista de economía institucional [En línea]. JUL-DIC 2008, No. 19, pp. 131-160. [Consultado el 11 de marzo de 2022]. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=2777479
- SÁNCHEZ, Silvia. Perfiles del ciberdelito: un campo de estudio inexplorado. Revista de Derecho [En línea]. AGO-DIC 2021, No. 30, pp. 67-76. [Consultado el 20 de julio de 2022]. Disponible en: https://www.lamjol.info/index.php/DERECHO/article/download/12223/14276/44901
- ZÚÑIGA, Laura. Modelos de Política Criminal frente a la Criminalidad Organizada: Entre eficacia y garantías. Revista Brasileira de Ciencias Políticas [En línea]. JUN-ABR 2020, No. 1, pp. 133-180. [Consultado el 22 de julio de 2022]. Disponible en: https://periodicos.pf.gov.br/index.php/RBCP/article/download/700/400/2717

Sitios Web:

- Biblioteca del Congreso Nacional de Chile. Efect os del agravamiento de las penas frente a la comisión de delitos. [En línea] [Consultado el 20 de julio de 2022]. Disponible en: https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/24913/1/Efectos_del_agravamiento_de_las_penas_frente_a_la_comision_de_delitos.pdf
- Cámara de diputados de Chile. Evaluación de la Ley. [En línea][Consultado el 24 de julio de 2022]. Disponible en: https://www.evaluaciondelaley.cl/leyes-evaluadas/
- Departamento de cooperación jurídica. Legislación sustantiva de delito cibernético. [En línea] [Consultado el 24 de julio de 2022]. Disponible en: http://www.oas.org/juridico/spanish/cybersp_legis.htm
- Diálogo de Derechos Humanos. La Convención de las Naciones Unidas Contra la Delincuencia Organizada Transnacional. [En línea] [Consultado el 21 de junio

de 2022]. Disponible en: https://dialogoderechoshumanos.com/blog/614-la-convencion-de-las-naciones-unidas-contra-la-delincuencia-organizada-transnacional

- Diccionario de la lengua española, Real Academia Española. Brujería. [En línea] [Consultado el 06 de abril de 2022]. Disponible en: https://dle.rae.es/brujer%C3%ADa?m=form
- Diccionario de la lengua española, Real Academia Española. Ciber. [En línea] [Consultado el 11 de marzo de 2022]. Disponible en: https://dle.rae.es/ciber-
- Diccionario de la lengua española, Real Academia Española. Demonología. [En línea] [Consultado el 06 de abril de 2022]. Disponible en: https://dle.rae.es/demonolog%C3%ADa
- Diccionario de la lengua española. Desarrollo. [En línea] [Consultado el 10 de julio de 2022]. Disponible en: https://dle.rae.es/desarrollo
- Diccionario económico. Delito. [En línea] [Consultado el 07 de abril de 2022]. Disponible en: https://economipedia.com/definiciones/delito.html
- Diccionario Jurídico de Derecho, Enciclopedia Jurídica. Delincuente. [En línea] [Consultado el 07 de abril de 2022]. Disponible en: http://www.enciclopedia-juridica.com/d/delincuente/delincuente.htm
- Diccionario Jurídico de Derecho, Enciclopedia jurídica. Ignorancia de la ley. [En línea] [Consultado el 24 de abril 2022]. Disponible en: http://www.enciclopedia-juridica.com/d/ignorancia-de-la-ley/ignorancia-de-la-ley.htm
- Diccionario Jurídico, La Voz del Derecho. Víctima. [En línea] [Consultado el 07 de abril de 2022]. Disponible en: https://lavozdelderecho.com/index.php/actualidad-2/corrup-5/item/2822-diccionario-juridico-concepto-de-victima-en-el-derecho-internacional
- Diccionario panhispánico de dudas. Ad hoc. [En línea] [Consultado el 28 de mayo de 2022]. Disponible en: https://www.rae.es/dpd/ad%20hoc
- Diccionario Panhispánico del español jurídico. Habeas data. [En línea] [Consultado el 10 de junio de 2022]. Disponible en: https://dpej.rae.es/lema/habeas-data#:~:text=1.,2.

- Diccionario Prehispánico del español jurídico. Consecuencia jurídica del delito. [En línea] [Consultado el 24 de abril de 2022]. Disponible en: https://dpej.rae.es/lema/consecuencia-jur%C3%ADdica-del-delito
- Diccionario Prehispánico del Español Jurídico. Control Social. [En línea] [Consultado el 07 de abril de 2022]. Disponible en: https://dpej.rae.es/lema/control-social
- Diccionario Prehispánico del Español Jurídico. Cooperación internacional. [En línea] [Consultado el 10 de julio de 2022]. Disponible en: https://dpej.rae.es/lema/cooperaci%C3%B3n-internacional
- El 19 Digital. Presidente Daniel Ortega: Aquí se está juzgando a criminales que han atentado contra el país. [En línea] [Consultado el 24 de julio de 2022]. Disponible en: https://www.el19digital.com/articulos/ver/titulo:117554-presidente-daniel-ortega-aqui-se-esta-juzgando-a-criminales-que-han-atentado-contra-el-pais
- INTERPOL. Fortalecimiento de Capacidades en Ciberdelincuencia en las Américas. [En línea] [Consultado el 20 de julio de 2022]. Disponible en: https://www.interpol.int/en/Crimes/Cybercrime/Cyber-capabilities-development/Cybercrime-Capacity-Building-in-the-Americas
- INTERPOL. INTERPOL refuerza la capacidad de vigilancia del delito cibernético en América Latina y el Caribe. [En línea] [Consultado el 20 de julio de 2022]. Disponible en: https://www.interpol.int/en/News-and-Events/News/2016/INTERPOL-boosts-cybercrime-policing-capacity-in-Latin-America-and-the-Caribbean
- Justia. Preguntas y respuestas sobre delitos informáticos. [En línea] [Consultado el 10 de junio de 2022]. Disponible en: https://mexico.justia.com/derecho-penal/delitos-informaticos/preguntas-y-respuestas-sobre-delitos-informaticos/
- Ministerio Público Fiscal de la Ciudad Autónoma de Buenos Aires. Cooperación internacional en materia de seguridad. [En línea] [Consultado el 15 de julio de 2022]. Disponible en: https://sistematizacion.com.ar/cuadernillos/oea/4/4.pdf
- OGDI. Historia del Cibercrimen. [En línea] [Consultado el 03 de marzo de 2022]. Disponible en: https://ogdi.org/historia-del-cibercrimen

- Policía Nacional. Oficiales concluyen con éxito capacitación en ciberdelitos. [En línea] [Consultado el 20 de julio de 2022]. Disponible en: https://www.policia.gob.ni/?p=61428
- SlideShare. Política criminal. [En línea] [Consultado el 04 de junio de 2021]. Disponible en: https://es.slideshare.net/fcokadir/politica-criminal
- Tn8. Encuentro en Nicaragua para conocer de ciberdelitos y seguridad digital. [En línea] [Consultado el 20 de julio de 2022]. Disponible en: https://www.tn8.tv/nacionales/533322-encuentro-en-nicaragua-para-conocer-de-ciberdelitos-seguridad-digital/
- UNICEF. ¿Qué es la adolescencia? [En línea] [Consultado el 20 de julio de 2022]. Disponible en: https://www.unicef.org/uruguay/que-es-la-adolescencia#:~:text=La%20Organizaci%C3%B3n%20Mundial%20de%20la,los%2010%20y%2019%20a%C3%B1os.
- UNODC. La ciberdelincuencia, en resumen. [En línea] [Consultado el 11 de marzo de 2022]. Disponible en: https://www.unodc.org/e4j/es/cybercrime/module-1/key-issues/cybercrime-in-brief.html

ANEXOS:

Tabla 1. *Modalidades del Cibercrimen según Fernando Miró.* En esta clasificación el autor distingue los ciberataques según los distintos intereses sociales afectados y la incidencia de las TICs en el fenómeno criminal.

	CIBERATAQUES PUROS	**CIBERATAQUES REPLICA**	**CIBERATAQUES DE CONTENIDO**
Cibercrímenes Económicos	• Hacking • Malware intrusivo • Malware destructivo • Ataques de insiders • Ataques DoS • Spam • Ciberocupación • Red • Antisocial networks	• Ciberfraudes (phishing, pharming, scam, auction fraud...) • Cyberspyware (uso de sniffers y demás spyware, ciberespionaje de empresa) • Identity theft • Spoofing (DNS spoofing, ARP spoofing, IP spoofing, web spoofing) • Ciberblanqueo de capitales • Ciberextorsión • Ciberocupación	• Distribución de pornografía infantil en internet • Ciberpiratería intelectual
Cibercrímenes Sociales		• Spoofing • Cyberstalking • Cyberbullying • Online harassment (ciberamenazas, coacciones, injurias, etc.) • Sexting (y extorsión con imágenes de sexting) • Online grooming	
Cibercrímenes Políticos	• Ataques DoS (cyberwar) • Ataques DoS (Cyberhacktivism) • Malware intrusivo	• Ciberespionaje terrorista • Ciberguerra	• Online hate speech • Ciberterrorismo (difusión de mensajes radicales con fines terroristas)

Tabla 2. *Cuadro comparativo de la regulación jurídica sustantiva en materia de ciberdelincuencia en los países de Nicaragua, Costa Rica y El Salvador.* En la siguiente tabla se evidencian contrastes entre la regulación jurídica sustantiva de Nicaragua, Costa Rica y El Salvador a razón de diversos elementos, tales como el ámbito de aplicación, el catálogo de ciberdelitos regulados o el objetivo perseguido por la norma.

	NICARAGUA	**COSTA RICA**	**EL SALVADOR**
Instrumento de regulación sustantiva	Ley 1042, Ley Especial de Ciberdelitos.	Código Penal.	Decreto No. 260, Ley Especial contra los delitos informáticos y conexos.
Terminología empleada	Delitos Cibernéticos/Informáticos (delitos relacionados con las TICs y los sistemas informáticos, cuya regulación se distingue por el fin, medio o método de comisión).	Delitos Informáticos y conexos (delitos relacionados con los sistemas informáticos cuya regulación es específica) y cibernéticos (delitos relacionados con las TICs cuya regulación se incluye como nueva modalidad de delitos tradicionales).	Delitos Informáticos y conexos (delitos relacionados con el uso de las tecnologías de la información y la comunicación y con los sistemas informáticos indistintamente).
Ámbito de aplicación	Será aplicable a todos los sujetos que cometan acciones, dentro o fuera del territorio nacional, utilizando los datos, sistemas informático o tecnologías de la información y la comunicación.	Se aplicará a quien cometa un hecho punible en el territorio de la República, salvo las excepciones establecidas en los tratados, convenios y reglas internacionales aceptados, incluyendo los hechos punibles cometidos en el extranjero regulados por el Código Penal.	Se aplicará a los hechos punibles cometidos total o parcialmente en el territorio nacional o en los lugares sometidos a su jurisdicción; también se aplicará a cualquier persona, natural o jurídica, nacional o extranjera, por delitos que afecten bienes jurídicos del Estado, de sus habitantes o protegidos por Pactos o Tratados Internacionales ratificados por El Salvador; incluyendo los actos cometidos en el extranjero de acuerdo a lo establecido en esta norma.
Objeto	Prevención, investigación, persecución y sanción de los delitos cometidos por	Prevenir y sancionar las acciones delictivas cometidas mediante el uso	Proteger los bienes jurídicos de aquellas conductas delictivas cometidas por medio de las

	medio de las Tecnologías de la Información y la Comunicación.	de las tecnologías de la información y la comunicación; y aquellas que involucren la utilización o que tengan como fin los sistemas informáticos.	Tecnologías de la Información y la Comunicación, así como su prevención y sancionamiento.
Tipologías delictivas	• **Ciberataques puros:** ○ Acceso indebido a los programas o datos informáticos. ○ Acceso indebido a sistemas informáticos. ○ Alteración, daño a la integridad y disponibilidad de datos. ○ Daño a sistemas informáticos. ○ Interceptación de comunicaciones y trasmisiones. ○ Interferencia del sistema informático o datos. ○ Violación de la seguridad del sistema informático. • **Ciberataques réplica:** ○ Acoso sexual. ○ Acoso. ○ Alteración, daño a la integridad y disponibilidad de datos. ○ Amenazas. ○ Captación indebida de comunicaciones ajenas. ○ Corrupción a personas	• **Ciberataques puros:** ○ Daño agravado. ○ Daño informático. ○ Instalación o propagación de programas informáticos maliciosos. ○ Instalación o propagación de programas informáticos maliciosos. ○ Suplantación de páginas electrónicas. • **Ciberataques réplicas:** ○ Acoso sexual en espacios públicos o de acceso público. ○ Amenaza a un funcionario público. ○ Corrupción de menores. ○ Difusión de información falsa. ○ Divulgación de información confidencial. ○ Espionaje informático. ○ Estafa informática. ○ Extorsión. ○ Facilitación de los medios para la	• **Ciberataques puros:** ○ Acceso Indebido a los Programas o Datos Informáticos. ○ Acceso Indebido a Sistemas Informáticos. ○ Alteración, Daño a la Integridad y Disponibilidad de los Datos. ○ Daños a Sistemas Informáticos. ○ Interceptación de Trasmisiones entre Sistemas de las Tecnologías de la Información y la Comunicación. ○ Interferencia de Datos. ○ Interferencia del Sistema Informático. ○ Secuestro de Sistemas, Programas o Datos Informáticos. ○ Violación de la Seguridad del Sistema. • **Ciberataques réplica:** ○ Acoso a Niñas, Niños y Adolescentes o Personas con Discapacidad.

	menores de 16 años o personas con discapacidad necesitada de especial protección. ○ Divulgación no autorizada. ○ Espionaje informático. ○ Falta a la confidencialidad. ○ Fraude informático. ○ Hurto por medios informáticos. ○ Manipulación de registros. ○ Manipulación fraudulenta de tarjetas inteligentes o instrumentos similares. ○ Obtención indebida de bienes o servicios por medio de tarjetas inteligentes o medios similares. ○ Posesión de equipos o prestación de servicios para vulnerar la seguridad informática. ○ Provisión indebida de bienes o servicios. ○ Provocación, apología e inducción a la comisión de delitos. ○ Revelación indebida de	consecución del delito informático. ○ Injurias. ○ Narcotráfico y crimen organizado. ○ Producción de material audiovisual. ○ Publicación de ofensas. ○ Sabotaje informático ○ Suplantación de identidad. ○ Trata de persona. ○ Turismo sexual. ○ Violación de correspondencia o comunicaciones. ○ Violación de datos personales. • **Ciberataques de contenido:** ○ Difusión de pornografía. ○ Fabricación, producción, o reproducción de pornografía. ○ Pornografía virtual y pseudo pornografía. ○ Tenencia de material pornográfico.	○ Acoso. ○ Corrupción de Niñas, Niños, Adolescentes o Personas con Discapacidad. ○ Espionaje Informático. ○ Estafa informática. ○ Extorsión sexual de niñas, niños y adolescentes o personas con discapacidad. ○ Falsedad de Documentos y Firmas. ○ Fraude Informático. ○ Hurto de Identidad. ○ Hurto por Medios Informáticos. ○ Manipulación de Registros. ○ Manipulación Fraudulenta de Tarjetas Inteligentes o Instrumentos Similares. ○ Obtención Indebida de bienes o servicios por medio de Tarjetas Inteligentes o Medios Similares. ○ Obtención y Divulgación No Autorizada. ○ Obtención y Transferencia de Información de Carácter Confidencial. ○ Posesión y uso de Equipos o Prestación de Servicios para la

	datos o información de carácter personal. ○ Suplantación informática. ○ Suplantación y apropiación de identidad informática. ○ Transferencia de información pública reservada. ○ Utilización de datos personales. ○ Violación de la custodia judicial de datos. • **Ciberataques de contenido:** ○ Propagación de noticias falsas. ○ Utilización de niñas, niños, adolescentes o personas con discapacidad necesitada de especial protección, en pornografía.		Vulneración de la Seguridad. ○ Provisión Indebida de Bienes o Servicios. ○ Revelación Indebida de Datos o Información de Carácter Personal. ○ Seducción de niñas, niños y adolescente o personas con discapacidad. ○ Técnicas de Denegación de Servicio. ○ Utilización de Datos Personales. • **Ciberataques de contenido:** ○ Adquisición o Posesión de Material Pornográfico de Niñas, Niños, Adolescentes o Personas con Discapacidad. ○ Intercambio de mensajes de contenido sexual con niñas, niños y adolescentes o personas con discapacidad. ○ Pornografía. ○ Utilización de Niñas, Niños, Adolescentes o Personas con Discapacidad en Pornografía.
	Penas privativas de libertad desde un año hasta diez años, las que	Penas privativas de libertad desde	

Consecuencias jurídicas	incluyen desde 100 días multa hasta 600 días multas como consecuencias accesorias; siendo la pena inferior de 200 a 300 días multa. Se regulan también agravantes comunes en casos determinados en donde la pena máxima será aplicada aumentada hasta en una tercera parte, junto con la inhabilitación del ejercicio de su profesión durante el tiempo que dure la pena.	seis meses hasta dieciséis años; siendo la pena mínima de diez a cincuenta días multa. Las penas se duplicarán cuando cualquiera de los delitos cometidos por medio de un sistema o red informática o telemática, o los contenedores electrónicos, ópticos o magnéticos afecte la lucha contra el narcotráfico o el crimen organizado.	Penas privativas de libertad desde un año hasta doce años; regulándose también agravantes comunes en casos determinados en donde la pena máxima será aplicada aumentada hasta en una tercera parte, junto con la inhabilitación del ejercicio de su profesión durante el tiempo que dure la pena.
Bienes jurídicos protegidos	Bines jurídicos individuales, colectivos y supraindividuales.	Bienes jurídicos individuales, colectivos y supraindividuales.	Bienes jurídicos individuales, colectivos y supraindividuales
Aspectos procesales	Medidas cautelares y procesales para la investigación, obtención y preservación de datos; e instrumentos de cooperación internacional. Riéndose en los demás de manera supletoria, por su Código Procesal Penal e instrumentos internacionales correspondientes.	Se rige por las disposiciones de su Código Procesal Penal e instrumentos internacionales en la materia.	No se establecen, rigiéndose por las disposiciones de su Código Procesal Penal, el cual fue reformado para la incorporación de apartados propios sobre delitos informáticos; e instrumentos internacionales en la materia.

Gráfico 1. *Procedimiento de evaluación legislativa ex post.* En este gráfico se muestran las etapas procedimentales de la evaluación ex post, incluyendo los elementos que deberán configurar cada una de ellas según las condiciones de eficacia instrumental.

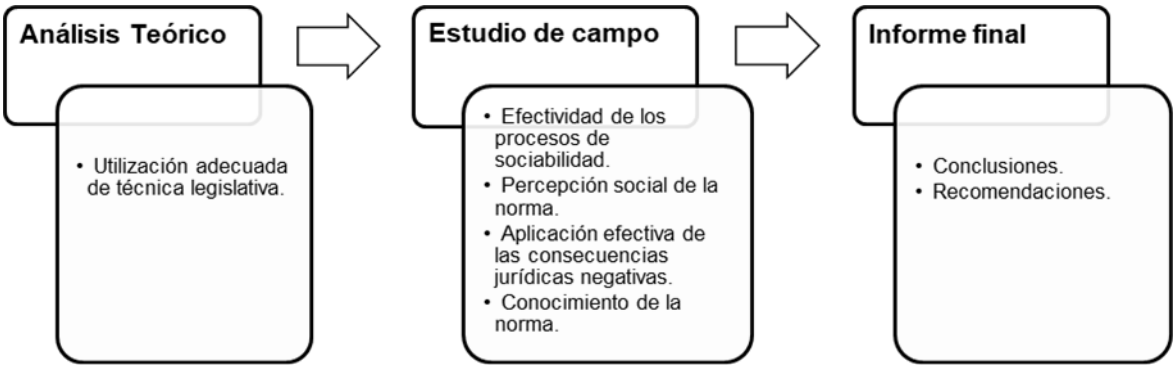


Gráfico 2. *Proceso de evaluación legislativa ex post.* En este gráfico se evidencian los tres elementos configurativos del proceso de evaluación *ex post*.

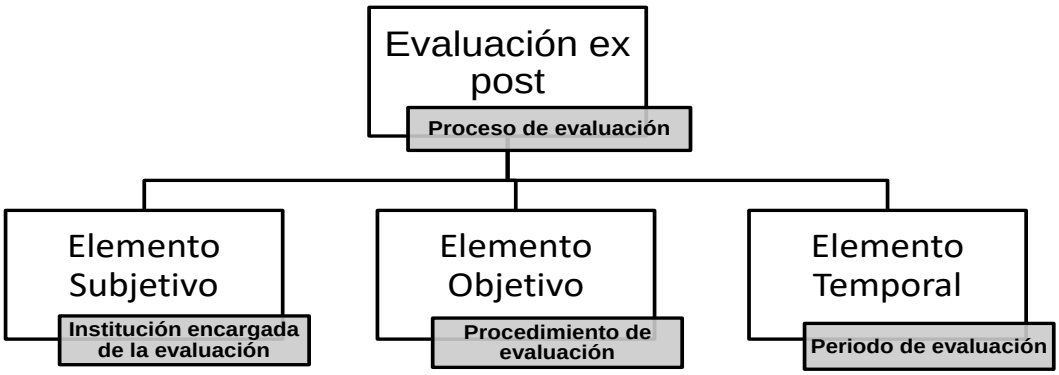


Gráfico 3. *Proceso penal nicaragüense*. En este gráfico se muestra el proceso penal ordinario nicaragüense, aplicable también a la materia ciberdelictual.

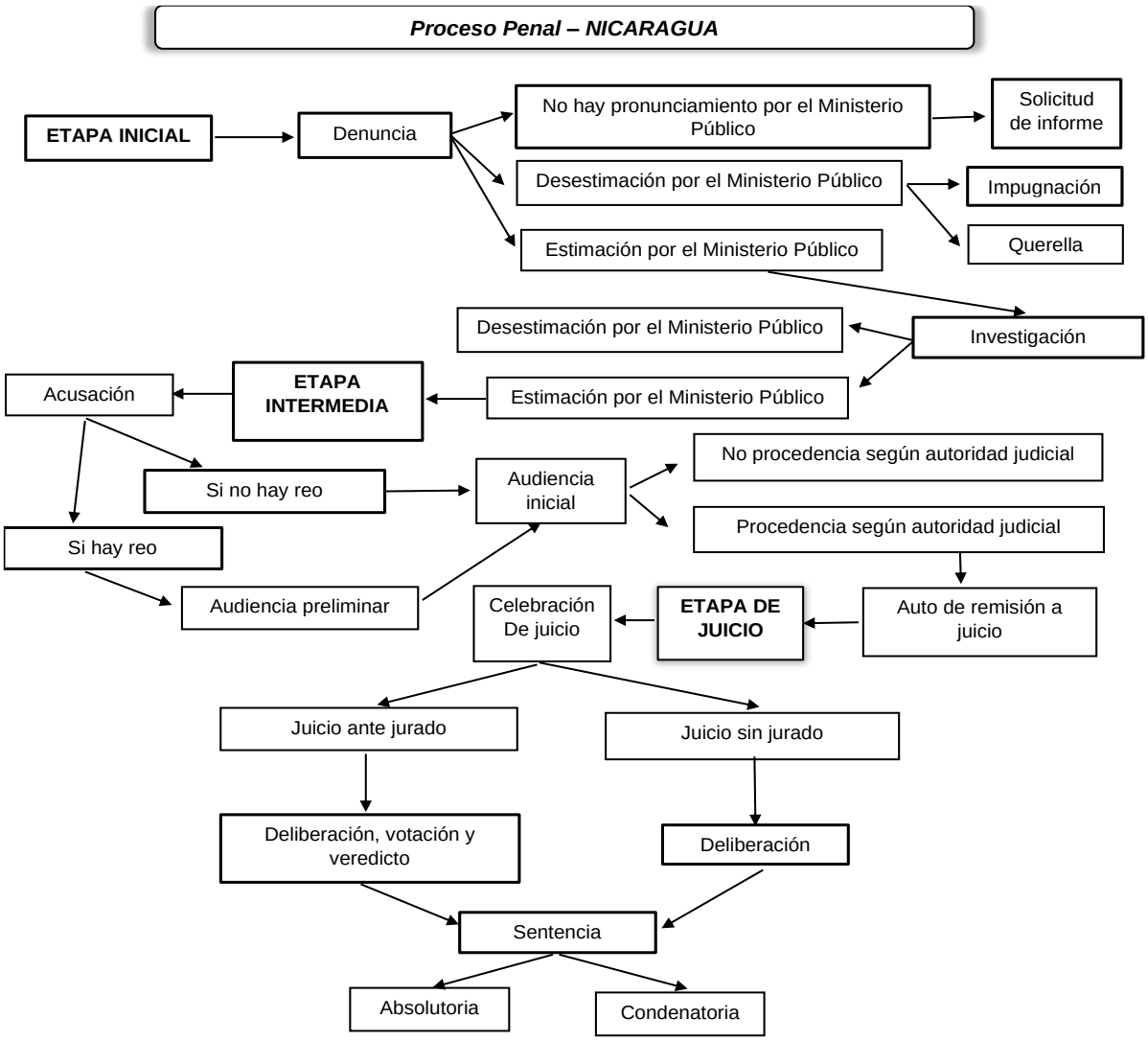


Gráfico 4. *Proceso penal costarricense.* En este gráfico se muestra el proceso penal ordinario costarricense, aplicable también a la materia ciberdelictual.

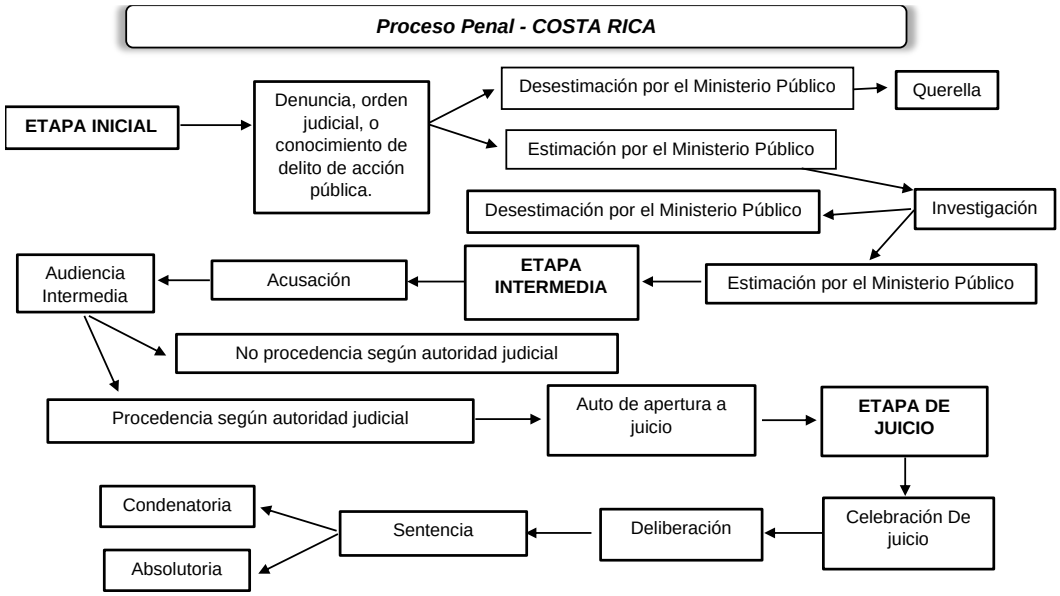


Gráfico 5. *Proceso penal salvadoreño*. En este gráfico se muestra el proceso penal ordinario salvadoreño, aplicable también a la materia ciberdelictual.