

UNIVERSIDAD NACIONAL AUTÓNOMA DE NICARAGUA

UNAN-LEÓN

AREA DE CONOCIMIENTO DE CIENCIAS JURÍDICAS Y SOCIALES.



MONOGRAFÍA PARA OPTAR AL TÍTULO DE LICENCIADO EN DERECHO.

ANÁLISIS JURÍDICO DE LOS CIBERDELITOS DE INDEMNIDAD, LIBERTAD E INTEGRIDAD SEXUAL CONTENIDOS EN LA LEY 1042, “LEY ESPECIAL DE CIBERDELITOS”.

AUTORES:

Br. Idalia Lucia Hernández Sánchez

Br. Freddy Omar Valladares Vanegas

TUTOR:

Msc. Guidyan Lenin Hernández García

León, Nicaragua, noviembre 2024

www.unanleon.edu.ni

2025:46/19 ¡Siempre más allá, Seguimos Avanzando en la Revolución!

RESUMEN

La presente investigación se titula **“Análisis jurídico de los ciberdelitos de indemnidad, libertad e integridad sexual contenidos en la Ley 1042, “Ley Especial de Ciberdelitos”**, y surge de la importancia de identificar los ciberdelitos, relacionados a la indemnidad, libertad e integridad sexual en la Ley 1042. Así como de la sentida necesidad por dar una repuesta más eficaz al avance de este tipo de criminalidad informática y de cómo el Derecho Penal debe responder en caso de que se consuman y cuál es el procedimiento que seguir. La presente investigación es de tipo teórica documental, con enfoque cualitativo, las fuentes de la información utilizadas son fundamentalmente los tratados internacionales, las leyes nacionales y la doctrina, y está dividida en tres acápite, en el primero describiremos los aspectos teórico-conceptuales que nos ofrece la doctrina general respecto al tema; en el segundo capítulo Identificaremos cuales son los ciberdelitos, relacionados a la indemnidad, libertad e integridad sexual en la Ley 1042, en el tercero observaremos el tratamiento procesal para los ciberdelitos, de indemnidad, libertad e integridad sexual en nuestro Derecho penal adjetivo , y por último expondremos las conclusiones y recomendaciones. Este trabajo está en pertinencia con las líneas de investigación de la Facultad de Ciencias Jurídicas proyectada para el área de las ciencias penales; con los ODS de la agenda 2030, específicamente con la educación de calidad, y paz, justicia e instituciones sólidas. y con los programas de integración Centroamericana y del Caribe.

CARTA DE APROBACIÓN DEL INFORME FINAL

León, 20 de noviembre del 2024.

Msc. Francisco Valladares Rivas

Subdirector

Área de CC.JJ.SS. UNAN-León.

S. D.

Estimado maestro:

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: **“Análisis jurídico de los ciberdelitos de indemnidad, libertad e integridad sexual contenidos en la Ley 1042, “Ley Especial de Ciberdelitos”, elaborado por los bachilleres: Idalia Lucia Hernández Sánchez y Freddy Omar Valladares Vanegas** de la carrera de Derecho a quienes previamente usted me asignó 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. Guidyan Hernández García

Académico del departamento de Derecho Público

ÍNDICE.

INTRODUCCIÓN	1
 CAPÍTULO I. GENERALIDADES DE LOS CIBERDELITOS	5
1.1.-Evolución histórica de los Ciberdelitos	5
1.2.- Evolución jurídica de los ciberdelitos	8
1.3.- Definiciones	12
1.4.- Naturaleza jurídica de los ciberdelitos.....	15
1.5.-Características de los Ciberdelitos.....	16
1.6.- Clasificación de los Ciberdelitos.....	19
1.7.- Elementos Teóricos básicos del Tipo Penal en los Ciberdelitos	22
1.7.1- Tipo Penal objetivo.....	23
A)-Sujeto Activo	23
B)-Sujeto Pasivo.....	23
C)-Acción Típica.....	24
D)- Bien Jurídico Tutelado.....	24
E)-Elementos accesorios	25
1.7.2- Tipo Penal Subjetivo	25
A)-Elemento subjetivo de autoría	26
B)- Dolo	26
C)- Imprudencia	27
 CAPÍTULO II. CIBERDELITOS CONTRA LA INTEGRIDAD, INDEMNIDAD Y LIBERTAD SEXUAL.....	28
2.1. TIPOS DELICTIVOS TIPIFICADOS EN LA LEGISLACIÓN NACIONAL	28
2.1.1- Utilización de niñas, niños, adolescentes o personas con discapacidad necesitada de especial protección, en pornografía a través del uso de las Tecnologías de la Información y la Comunicación.....	29

2.1.2	Corrupción a personas menores de 16 años o personas con discapacidad necesitada de especial protección a través del uso de las Tecnologías de la Información y la Comunicación	32
2.1.3.	Acoso a través del uso de las Tecnología de la información y la comunicación	34
2.1.4.	Acoso sexual a través del uso de las Tecnologías de la Información y la Comunicación	37
2.2.	TIPOS DELICTIVOS CALIFICADOS COMO CIBERDELITOS NO TIPIFICADOS EN NICARAGUA.....	39
1.1.	Cyberbullying	39
2.3.	Sexting.....	41
2.4	Sextorsión.....	43
2.5.	Grooming	44

CAPÍTULO III. ASPECTOS PROCESALES DE LOS CIBERDELITOS RELACIONADOS A LA INTEGRIDAD, INDEMNIDAD Y LIBERTAD SEXUAL

3.1.	Jurisdicción	48
3.2.	Competencia.....	49
3.3.	Mediación	51
3.4.	Procedimiento.....	55
3.5.	Procedimiento Ordinario Por Delitos Graves	56
3.6.	Medidas de aseguramiento y técnicas de investigación	59
3.7.	Conservación De Datos	62
3.8.	Conservación de datos de contenido.....	64
3.9.	Conservación de datos de tráfico	65
3.10	conservación de datos abonados	67
3.11.	Aspectos Generales de la Prueba	68
3.12.	Características de los medios de prueba.....	70
3.13.	Elementos de convicción	71
3.14.	Naturaleza Jurídica de la prueba en los Ciberdelitos.....	72

DISEÑO METODOLÓGICO.....	74
CONCLUSIONES	77
FUENTES DE LA INVESTIGACIÓN.....	78

I- INTRODUCCIÓN.

El objeto de la presente investigación es el estudio de los delitos informáticos relacionados con la libertad e integridad Sexual, para ello nos propusimos como objetivo general Analizar los Ciberdelitos de indemnidad, libertad e integridad sexual contenidos en la ley 1042, “Ley Especial de Ciberdelitos”, y como objetivos específicos los siguientes: establecer el marco conceptual del tipo penal ciberdelitos y su proceso evolutivo desde sus orígenes hasta la actualidad; Identificar los ciberdelitos, relacionados a la indemnidad, libertad e integridad sexual en la Ley 1042 y por último explicar el tratamiento procesal para los ciberdelitos, de indemnidad, libertad e integridad sexual en nuestro Derecho Penal adjetivo.

El auge y la aceptación masiva de las Tecnologías de la información y la comunicación (TICs) ligado al fácil acceso y manejo, constituyen un nuevo fenómeno jurídico, que representa nuevos riesgos delictivos, para una sociedad globalmente interconectada, todo debido al rol tan fundamental, que tienen el uso de estas tecnologías en nuestro vivir cotidiano¹.

Considerando que en el quehacer diario, es natural, casi vital el uso de algún aparato o dispositivo electrónico para ejecutar tareas que en otros tiempos se efectuaban manualmente, su uso se ha convertido en un necesidad, por lo que la integración tecnológica, en definitiva, ha marcado lo que comúnmente se ha denominado la nueva “era digital”, capaz de procesar, almacenar y comunicar en gran medida grandes cantidades de información, innovando significativamente todos los ámbitos, tanto económico, social o cultural, acelerando y trasformando así los límites entre actividades laborales y simples tareas cotidianas.

Desde esta perspectiva las TICs y su plenitud aportan globalmente, muchos efectos positivos, en especial para esta sociedad tan moderna, sin embargo, su mal uso,

¹ MIRO LLINARES, Fernando, delincuencia asociada al uso de las TIC, [en línea], Universidad abierta de Cataluña, España, 2013 [fecha de consulta: 25 de agosto del 2023]. Disponible en: <https://openaccess.uoc.edu/>.

adherido a su popular aceptación, a escala global, incrementa una variedad típica de comportamientos que materializan riesgos y amenazas de carácter informático.

El alcance masivo de estos aparatos tecnológicos, en una sociedad de este calibre advierte un incremento en la ola delictiva a nivel mundial, creando vulnerabilidad, haciendo que el cibercrimen se escape de lo tradicional en el Derecho Penal, pues actúa bajo un nuevo entorno digital que traspasa lo que conocemos, y que se podría traducir en una ampliación de Derechos, por lo que resulta una responsabilidad Estatal garantizar seguridad informática. Esto requiere una verdadera intervención jurídica que garantice seguridad informática y con este estudio se pretende precisar, en los aportes tan autónomos e innovadores que comprenden los Ciberdelitos, respecto a los comportamientos realizados a través de las TICs, y que representan graves riesgos a la sociedad, centrándonos especialmente en los delitos relacionados a la indemnidad, integridad y libertad sexual, que acoge nuestra legislación en la Ley 1042 “Ley especial de ciberdelitos” capítulo V.

La Ley 1042 “Ley Especial de Ciberdelitos” introduce y tipifica algunos delitos de forma amplia y general, pero no advierte, ni prevé; que el uso de las tecnologías y su evolución, en caso de un mal manejo, puede complicar la persecución de estos tipos delictivos, valorando las características propias de estos delitos, determinadas acciones y omisiones, de conductas, se escapan de la realidad procesal penal, al no contemplar mediante un procedimiento amplio y específico la persecución de estos delitos . Por todo lo anterior nos hemos planteado las siguientes preguntas de investigación: ¿Cómo debe el Derecho Penal enfrentar la comisión de los ciberdelitos en relación con la libertad, integridad e indemnidad sexual? ; ¿Esta Ley está cumpliendo con su función de regular las diferentes formas de delitos cibernéticos, contra los derechos de indemnidad, integridad y libertad sexual para proteger a las personas? ; ¿Existen Delitos sexuales que no están contemplados en la Ley 1042? ; ¿Cuáles son los factores que obstaculizan el debido cumplimiento de la norma? Y ¿Es necesario incluir en la ley 1042 los tipos penales que se utilizan a nivel internacional y que no están contemplados en nuestra Ley de ciberdelitos?

La justificación de la escogencia de este tema dentro del marco del Derecho Penal obedece a varios factores, el primero de ellos es su vigencia en la actualidad, ya que a diferencia de otros temas ya trillados, estancados o en desuso, los delitos abordados en nuestro tema han evolucionado a través del tiempo, se han adaptado a la perfección a los cambios sociales, jurídicos e informáticos, el segundo factor es su gran importancia, pues no se puede negar que el flagelo del cibercrimen es una realidad principalmente los delitos relacionados con la libertad, integridad e indemnidad sexual, y por último nos hemos planteado aportar con nuestro estudio el identificar los vacíos que presenta el capítulo V de la Ley 1042, en pro de aportar nuestras recomendaciones jurídicas pertinentes y que estemos en armonía a nivel internacional para poder combatir eficazmente este flagelo de los ciberdelitos.

La presente investigación está estructurada en tres capítulos, en el primero describiremos los aspectos teórico-conceptuales que nos ofrece la doctrina general respecto al tema, en el segundo capítulo Identificaremos cuales son los ciberdelitos, relacionados a la indemnidad, libertad e integridad sexual en la Ley 1042, en el tercero observaremos el tratamiento procesal para los ciberdelitos, de indemnidad, libertad e integridad sexual en nuestro Derecho penal adjetivo, y por último expondremos las conclusiones y recomendaciones.

La metodología utilizada en la presente investigación consistió tanto en el método analítico deductivo, como el de análisis síntesis, dado que se pretende partir del estudio de lo general a lo particular, a fin de garantizar su correcta síntesis, mediante conclusiones válidas. La presente investigación es de tipo teórica documental con enfoque cualitativo.

Las fuentes de la información utilizadas son como fuentes primarias los tratados internacionales y leyes nacionales, como fuentes secundarias la doctrina y como fuentes terciarias páginas web oficiales las cuales son fundamentales para la técnica utilizada fue la revisión documental.

Este trabajo investigativo compete al área de Democracia, Gobernabilidad y Seguridad Ciudadana, en concordancia con el Plan Nacional de Desarrollo Humano Sostenible de

la Republica de Nicaragua; a los Objetivos de Desarrollo Sostenibles (ODS), a los programas de integración Centroamericana y del Caribe y a las líneas de investigación en el área de ciencias penales aprobadas por la Facultad de Ciencias jurídicas y Sociales de la UNAN-León.

CAPÍTULO I: GENERALIDADES DE LOS CIBERDELITOS.

1.1. Evolución histórica de los Ciberdelitos.

La creación de nuevas tecnologías, como nuevo medio de la comunicación, y las personas, trae aparejado nuevas posibilidades para su aprovechamiento indebido e ilícito. Desde la creación del telégrafo y posteriormente la incorporación del teléfono a la vida cotidiana, la irrupción de la computadora personal, la expansión de Internet y la World Wide Web. La capacidad de procesamiento de datos e información y el acceso a miles de personas en un medio interactivo, de características globales amplió las posibilidades de comisión de hechos ilícitos e ilegales a partir del fácil manejo en el surgimiento de entornos digitales “amigables” y aplicaciones prácticas y de sencillo manejo, así como las posibilidades de anonimato en las comunicaciones.²

Durante la década de 1970 se comienzan a registrar una serie de casos que arrojan pérdidas cuantiosas para los sectores privados. A partir del desarrollo de delitos económicos como el espionaje informático, la piratería de software, el sabotaje y la extorsión. En relación con el espionaje, estos se llevaban a cabo mediante la copia directa desde los dispositivos informáticos, el robo directo de los mismos para la extracción de información -discos duros, diskettes-, y la absorción de emisiones electromagnéticas para captar datos. El objeto del delito eran los programas de computación, los datos de investigación en el área de defensa, la información contable de las empresas y la cartera de direcciones de clientes corporativos. En relación con la piratería de software, la modalidad característica era la copia no autorizada de programas de computadora para su comercialización en el marco de espionaje industrial.³

Para los casos de sabotaje y extorsión informática, estos eran los delitos que más preocupaban a las administraciones gubernamentales y empresas ante la alta concentración de datos almacenados electrónicos. Los objetivos eran tanto bienes tangibles -dispositivos físicos como intangibles -datos e información- afectando tanto

² SAIN, Gustavo. Evolución Histórica de los delitos informáticos. *Revista pensamiento penal [en línea]. 2015, abril* [fecha de consulta: el 28 de abril del 2023]. ISSN: 1853- 4554. Disponible en : [Evolución histórica de los delitos informáticos | Revista Pensamiento Penal](#).

³ Ídem.

hardware como de software en los dispositivos. En relación con los daños físicos, durante los años 70 se registraron casos de uso de bombas caseras en instalaciones y dispositivos informáticos de empresas por distintos problemas laborales. En relación con los fraudes financieros producidos a partir del uso de nuevas tecnologías, los primeros casos se empezaron a producir en Estados Unidos a finales de la década de 1970 a partir de los fallos en los sistemas de seguridad de las redes y la inexperiencia de los administradores de dichos sistemas. El modus operandi, se relacionaba con la manipulación de facturas para pagos de salarios de personal y los balances de pagos de los bancos.⁴

A partir de los primeros años de la década de 1980, los delitos informáticos adquieren una importante notoriedad a partir de un aumento exponencial de fraudes y el tratamiento de la problemática por parte de organismos internacionales. Para el caso de los fraudes, los casos típicos se realizaban mediante la manipulación de uso de tarjetas de débito en cajeros automáticos, fundamentalmente a través de la vulneración de las bandas magnéticas. Esto motivó la utilización por parte de las empresas emisoras de la adopción de chips en los plásticos como medida de seguridad. Fue justamente durante esta época donde comienza la protección normativa de los países europeos a los bienes inmateriales como el dinero electrónico, proceso iniciado por Estados Unidos en 1978. La cobertura legal de las bases de datos de las instituciones bancarias y empresas resultaba indispensable para la realización de negocios, fundamentalmente contra el robo de información comercial.⁵

A fines de esa década comenzaron a aparecer contenidos ilícitos y nocivos en las redes tales como amenazas contra las personas, incitación al odio y el intercambio de material de pornografía infantil, tanto, así como actos de violencia y discriminación racista por parte de grupos extremistas.⁶

Con la apertura global de Internet a mediados de los 90s por parte de la administración norteamericana y el posterior desembarco de las empresas y bancos a la red para el

⁴ Ibid. P.2.

⁵ Ibid. P.3.

⁶ Ídem.

desarrollo del comercio electrónico, la preocupación central pasaba por el desarrollo de estándares de encriptación seguros para el desarrollo de operaciones financieras y la compraventa de productos en línea. Asimismo, la industria discográfica y cinematográfica comenzó una afrenta contra la multiplicidad de casos de violaciones a los derechos de autor a partir de la descarga e intercambio en línea de música y películas bajo leyes de copyright⁷, lo que generó un debate acerca de cómo concertar acciones de cooperación internacional para evitar fugas del negocio. La difusión de imágenes y/o ofrecimiento de servicios sexuales de menores en la Web alertaban a las autoridades de los países sobre la ola de pedofilia que asomaba a partir de casos de grooming o acoso sexual a menores en línea. El tema de la protección a la intimidad y la privacidad se empezaron a debatir mediante el uso de nuevas tecnologías.⁸

La difusión de imágenes y ofrecimiento de servicios sexuales de menores en la Web alertaban a las autoridades de los países sobre la ola de pedofilia, que asomaba a partir de casos de grooming o acoso sexual a menores en línea. El tema de la protección a la intimidad y la privacidad, se empezaron a debatir mediante el uso de nuevas tecnologías.

La expansión y generalización de Internet ha provocado, a la vez, la aparición de un elenco de actividades nocivas para los ciudadanos, algunas de ellas producen lesiones de bienes jurídicos relevantes, protegidos por el Derecho penal. Por lo general, un número importante de estas actividades constituye una peculiar adaptación al espacio virtual, de conductas lesivas más o menos clásicas desde la perspectiva penal, para cuya ejecución se aprovecha ahora la viralidad y globalidad de este canal de comunicación digital (como ocurre, por ejemplo, con las estafas).

Ahora bien, Internet ha convertido de igual forma, una serie de conductas residuales en hechos delictivos masivos, como sucede con la pornografía infantil, habiendo sacado a la luz una ingente demanda de este tipo de materiales.

⁷ Real Academia Española. “*Diccionario de la lengua española*” [en línea] [fecha de consulta: el 31 de julio del 2023]. Disponible en: <https://dle.rae.es/>.

⁸ SAIN, Gustavo. Loc. Cit. Pp.3-4.

Muchos actos ilícitos ya tipificados en el Código Penal se consuman bajo esta modalidad criminal tecnológica, convirtiéndose así en un instrumento, no solo para los cibercriminales, pues su uso cotidiano si bien produce considerables beneficios, en la misma medida es una herramienta peligrosa, fácilmente se convierte un portal factible y rápido para ejecutar cualquier actividad delictiva.

Por ejemplo; el acoso virtual. Ya no es el clásico caso, en el que el acosador tiene que estar cerca o perseguir a la víctima. Valiéndose de la tecnología, el acosador actúa por medio de celulares, computadoras o redes sociales, perturbando constantemente a la posible víctima, sin necesidad de estar cerca; facilitándole así, desarrollar un patrón delictivo reiterado y constante.

1.2. Evolución jurídica de los ciberdelitos.

Es debido a la fácil aceptación y auge que portan el desarrollo de las TICs⁹ lo que ha incrementado significativamente, la criminalidad y a causa de ser las mismas el medio de perpetración de estos delitos, insta a los Estados, en intervenir y proteger a la sociedad.

El primer Convenio del Consejo Europeo o Convenio de Budapest, retoma ese nombre por haberse celebrado en ese lugar y fue adoptado en noviembre del 2001 y entro en vigor en el 2004. Este Convenio es el único que aborda el tema de los ciberdelitos o cibercriminal; está abierto para que pueda ser adoptado por cualquier país del mundo; cabe destacar que 56 países se han adherido¹⁰.

El Convenio de Budapest consta de 48 artículos divididos en cuatro capítulos, con sus respectivas secciones. El primer capítulo se encarga de definir términos como "sistema informático" "dato informático" "proveedor de servicio" y "datos de tráfico". El segundo capítulo se encarga de establecer las medidas que deben ser tomadas a nivel nacional por los Estados parte, obtención en tiempo real de datos de tráfico o interceptación de contenido. En este apartado, el convenio establece la necesidad de criminalizar

⁹Siglas de Tecnología de Información y Comunicación (TICs)

¹⁰ QUEZADA SALDAÑA, Martha Lorena. *"Análisis jurídico de la ley 1042: "Ley especial de ciberdelitos"*. Managua, 2021. P.19

determinadas conductas que se realizan mediante dispositivos tecnológicos. Entre ellas están: el acceso ilícito a un sistema informático, la interceptación ilícita de datos, el abuso de dispositivos, el fraude informático y delitos relacionados con pornografía infantil y propiedad intelectual. El tercer capítulo trata sobre cooperación internacional y establece disposiciones sobre asistencia mutua en temas como extradición o acceso, conservación, obtención en tiempo real e interceptación de datos. El capítulo final se refiere a cuestiones de entrada en vigor, forma de adhesión de los estados y las reservas que pueden hacerse al momento de incorporarse¹¹.

La Organización de las Naciones Unidas (ONU en el 8º Congreso de las Naciones Unidas sobre prevención del delito y tratamiento del delincuente (celebrado en La Habana, Cuba, del 27 de agosto al 7 de septiembre de 1990), la Asamblea General de Naciones Unidas adoptó una Resolución que tenía por objeto la legislación contra el ciberdelito. Basándose en esta Resolución las Naciones Unidas publicaron en 1994 un Manual sobre la prevención y el control de delitos informáticos.¹²

En el 2000 la Asamblea General aprobó una Resolución sobre la lucha contra la utilización de la tecnología de la información con fines delictivos. En esta Resolución la Asamblea General específica, una serie de medidas destinadas a combatir la utilización indebida a la tecnología de la información, por ejemplo: Los Estados deben velar por que en su legislación y práctica se eliminan los refugios seguros para quienes utilicen la tecnología de la información con fines delictivos. Debe coordinarse entre todos los Estados interesados la cooperación, en lo que se refiere a la vigilancia del cumplimiento de la Ley, y la investigación y el enjuiciamiento de los casos en que se utilice la tecnología de la información, con fines delictivos en el plano internacional. El personal encargado de hacer cumplir la Ley debe contar con capacitación y equipo adecuado para hacer frente a la utilización de la tecnología de la información con fines delictivos.¹³

¹¹ Ídem.

¹² Ídem. P. 20.

¹³ Ídem. P.20.

En 2014, la Conferencia de ministros de Justicia de los Países Iberoamericanos (COMJIB)¹⁴ suscribió el Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en materia de Ciberdelincuencia. Nicaragua en el año 2020 aprobó dicho convenio¹⁵ que tiene por objeto reforzar la cooperación mutua de las Partes, para la adopción de medidas de aseguramiento y obtención de pruebas para la lucha contra la ciberdelincuencia, así como la Recomendación relativa a la Tipificación y Sanción de la Ciberdelincuencia. Los instrumentos han sido suscritos por México, Guatemala, Nicaragua, Portugal, Perú y Uruguay y firmado por Argentina.

Los instrumentos precitados representan el mayor avance regional, en cuanto a la atención señalada a esta problemática. Derivado de las carencias que las leyes penales iberoamericanas respecto de los tipos penales referidos al ciberdelito, y al hecho de que estas lagunas, permiten tanto a la delincuencia individual, como a la organizada lesionar o poner en grave peligro los bienes jurídicos esenciales con el propósito de establecer criterios mínimos y comunes en la prevención y luchas contra el ciberdelito, y sin menoscabar los avances alcanzados en los respectivos ordenamientos jurídicos así como las obligaciones internacionales asumidas por cada Estado, la COMJIB recomienda armonizar, en el marco de las políticas criminales de cada país, leyes penales sustantivas que tipifiquen las conductas que se describen a continuación, en aras de lograr una mayor eficacia en la prevención, persecución y sanción de dichos ilícitos, para facilitar la cooperación judicial, entre los distintos países y tratar de impedir la existencia de espacios de impunidad. El Convenio de Budapest es compatible con otros instrumentos internacionales, como el Convenio del Consejo de Europa sobre la Ciberdelincuencia.¹⁶

Es bien sabido que la manifestación de la globalización sumada al fenómeno cibernético origina un proceso de integración y desarrollo en todos los ámbitos, uniendo mercados,

¹⁴ La Conferencia de ministros de Justicia de los Países Iberoamericanos (COMJIB) es una organización internacional de carácter intergubernamental. Su objeto es el estudio y promoción de formas de cooperación jurídica entre los Estados miembros.

¹⁵ Decreto A.N. No. 86551. "Decreto de aprobación del convenio Iberoamericano de cooperación sobre investigación, aseguramiento y obtención de prueba en materia de ciberdelincuencia". En la Gaceta diario oficial, del 03 de marzo del 2020.

¹⁶ QUEZADA SALDAÑA, Martha Lorena. Loc. Cit. Pp. 23 - 24.

sociedades y culturas. Centrándonos propiamente en la interconexión a través del internet, el constante flujo de información que provoca influencias de unas culturas sobre otras, esta característica, simplifica el canal o el medio en que se pueden cometer delitos.

A consecuencia de estas relaciones mundiales, en razón a esta facilidad y considerando la conducta y el medio delictivo del sujeto activo, que solo necesita estar detrás de cualquiera aparato tecnológico, desde los conocimientos más suficientes hasta los más básicos, y a la distancia de un clic entre un país a otro, lo que constituye una verdadera responsabilidad jurídica de parte de las naciones, para acceder hasta el sujeto pasivo. Dicha circunstancia podría ser un reto de consideración al momento de crear los diversos instrumentos jurídicos, que evidencien y puedan procesar judicialmente a los actores de estos crímenes.

Debido a la problemática causada por el desarrollo de las Tecnologías de Informática y Comunicación, nuestros legisladores crean la Ley 1042, “Ley Especial de Ciberdelitos” aprobada por la Asamblea Nacional el 27 de octubre de 2020 y publicada en la Gaceta Diario Oficial el 30 de octubre del año 2020, misma que entró en vigor el 30 de Diciembre del año 2020, tutelando los Derechos fundamentales de los ciudadanos Nicaragüenses en relación a la intimidad de las personas, sus datos, su información, la inviolabilidad de su correspondencia, comunicación, su patrimonio, libertad e Integridad sexual, todos derechos humanos de rango constitucional.

Anterior a su aprobación, no existía una normativa propiamente especializada en la regulación de los Derechos informáticos relacionados a la libertad e integridad sexual, pero con la Ley 1042 se integran nuevos términos, al derecho penal y nuestra legislación, procurando así la protección de Derechos de la sociedad nicaragüense y por ende de las personas más vulnerables.

Previa a la existencia de la Ley 1042, los delitos informáticos eran tratados como delitos comunes según los casos en que se podían por decirlo así “encasillar” bajo la figura de la propalación que el Código Penal establece. Al no existir una Ley especializada que

tipifique exclusivamente estos delitos, se procesaba en la medida que el art 175¹⁷ del Código Penal establece, dejando por fuera la tipificación a las víctimas de este tipo de delitos, enviando muchas veces, casos al desecho, todo porque no se podía tomar como delito a falta de la tipicidad que el título II capítulo II, le dedica en el Código Penal, referido a las conductas que son consideradas delitos contra la libertad e integridad sexual.

1.3. Definiciones.

➤ Ciberdelitos o Delito informático.

Según la Real Academia Española son ...“infracciones penales cometidas utilizando un medio o instrumento informático.”... ¹⁸, podríamos definir que los ciberdelitos son todas aquellas acciones típicas, establecidas como delitos que utilizan medios tecnológicos de información que facilite su producción, es decir son el puente para la consumación del delito.

Por su parte el autor mexicano Julio Téllez Valdés¹⁹, señala que los delitos informáticos, son actitudes contrarias a los intereses de las personas, en que se tiene a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin (concepto típico).

La ley 1042, Ley Especial de Ciberdelitos, en su artículo. 3 numeral cuatro, define los Ciberdelitos como: “...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 Ley No. 641, “Ley de Código Penal de Nicaragua”. SENICSA. Abril. 2015. P. 76. ... **“Art. 175 Explotación sexual, pornografía y acto sexual con adolescentes mediante pago.”**

¹⁸ Real Academia Española. “*Diccionario panhispánico del español jurídico*” [en línea] [fecha de consulta: 02 de agosto del año 2023]. Disponible en: <https://dpej.rae.es/lema/delito-inform%C3%A1tico>.

¹⁹ VALDÉS TÉLLEZ, Julio. “*Derecho informático*”. 4ª ed. México: Mc Graw Hill Interamericana Editores, 2004. ISBN 9701043065. P.188.

➤ **Cibercrimen.**

El término cibercrimen se puede referir a cualquier actividad delictiva que implique un ordenador, ya sea la herramienta del crimen o su objetivo. De acuerdo con el Departamento de Justicia, todo cibercrimen se puede organizar en tres categorías; crímenes que usan ordenadores como armas (por ejemplo, ataques de hackers), crímenes que atacan un ordenador u otro dispositivo (por ejemplo, para acceder a una red) y crímenes en los que el ordenador no es la herramienta principal, pero aun así juega un papel importante (por ejemplo, almacenar archivos descargados ilegalmente).²⁰

Tal y como ocurre con las actividades criminales fuera de la red, la mayoría de los perpetradores de los actos cibercriminales están motivados por las ganancias económicas. Además de dinero, también les mueven sus egos, una causa en la que creen, venganzas personales, sentido de notoriedad, así como el deseo de mejorar su estatus en los círculos de hackers.²¹

➤ **Dispositivos.**

Es cualquier mecanismo, aparato, medio que se utiliza o puede ser utilizado, para realizar cualquier función de la tecnología de información y comunicación, ya sean estos, celulares, computadoras, tabletas, siempre que puedan mantener una conexión de cualquier tipo, ya sea de red, o a la internet.

➤ **Ciberespacio.**

El ciberespacio constituye un escenario táctico, estratégico y operativo diferente de los espacios terrestre, marítimo, aéreo y exterior que ha sido calificado en la doctrina como uno de los *global commons*²². Es un entorno complejo resultante de la interacción entre

²⁰ SoftwareLab.Org. “¿Qué es el cibercrimen? La definición y los 5 tipos principales.” [en línea] [fecha de Consulta: 08 de junio del 2023]. Disponible en : [¿Qué es cibercrimen? La definición y los 5 tipos principales \(softwarelab.org\)](https://softwarelab.org)

²¹ Ídem.

²² “Patrimonio mundial”, [en línea] [fecha de consulta: 02 de agosto del año 2023]. Disponible en: <https://www.deepl.com/es/translator#en/es/Global%20Commons>.

las personas, el software y los servicios en Internet por medio de dispositivos tecnológicos (TIC) conectados a redes, el cual no existen en ningún tipo de forma física.²³

➤ **Internet.**

Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación.²⁴

➤ **Usuario.**

En informática se entiende por usuario, el conjunto de características o preferencias que la persona tiene sobre sus búsquedas de Internet o en los sitios Web que frecuenta. Y es con base a los datos que introduce a través de los diversos sitios, como se va conformando dicho perfil.²⁵

➤ **Red.**

Conjunto de computadoras o de equipos informáticos conectados entre sí y que pueden intercambiar información.²⁶

Son los sistemas de comunicación que conectan varios equipos y se componen básicamente de usuarios, software y hardware. Entre sus ventajas está el compartir recursos, intercambiar y compartir información, homogeneidad en las aplicaciones y mayor efectividad.²⁷

➤ **Redes sociales.**

²³ ALBARRÁN RUFIAN, Mikel. “La importancia del ciberespacio y de la seguridad en las organizaciones”. [en línea] [fecha de consulta: 6 de agosto de 2023]. Disponible en: https://www.segurilatam.com/tecnologias-y-servicios/ciberseguridad/la-importancia-del-ciberespacio-y-de-la-ciberseguridad-en-las-organizaciones_20200831.html.

²⁴ Real Academia Española. “Diccionario panhispánico del español jurídico” [en línea] [fecha de consulta: 03 de agosto del año 2023]. Disponible en: <https://dle.rae.es/internet?m=form>.

²⁵ El perfil del usuario. Boletín UPIITA El camino a la innovación educativa. No. 39. México. [en línea] [consultado el 6 de agosto de 2023]. INSS 2007-6150. Disponible en: <http://www.boletin.upiita.ipn.mx/index.php/ciencia/510-cyt-numero-39/338-el-perfil-de-usuario>.

²⁶ Real Academia Española: “Diccionario panhispánico del español jurídico” [en línea] [fecha de consulta: 03 de agosto del año 2023]. Disponible en: <https://dle.rae.es/red?m=form>.

²⁷ CLARO, Colombia. [en línea] [fecha de Consulta: 06 de agosto de 2023]. Disponible en: <https://www.claro.com.co/institucional/que-son-las-tic/>

Servicio de la sociedad de la información que ofrece a los usuarios una plataforma de comunicación a través de internet para que estos generen un perfil con sus datos personales, facilitando la creación de comunidades con base en criterios comunes y permitiendo la comunicación de sus usuarios, de modo que pueden interactuar mediante mensajes, compartir información, imágenes o vídeos, permitiendo que estas publicaciones sean accesibles de forma inmediata por todos los usuarios de su grupo.²⁸

➤ Tecnologías de Información y comunicación (TIC)

Son tecnologías que utilizan la informática, la microelectrónica y las telecomunicaciones para crear nuevas formas de comunicación a través de herramientas de carácter tecnológico y comunicacional, esto con el fin de facilitar la emisión, acceso y tratamiento de la información.²⁹

1.4.- Naturaleza jurídica de los ciberdelitos.

Según el Prof. Montoya³⁰ catedrático de Informática jurídica en la Universidad central de Medellín Colombia. El Derecho informático tiene naturaleza mixta, ya que es un Derecho público cuando se refiere a tres campos específicos, a saber: La regulación internacional de datos informatizados (aspecto internacional público), libertad informática y defensa de otras libertades individuales frente a eventuales agresiones provenientes de la tecnología informática (aspecto constitucional) y la delincuencia informática (derecho penal. Es derecho privado cuando se refiere a la contratación informática (Contratos cuyos objetos sean elementos de Hardware o Software), protección de software y comercio electrónico.

El nuevo ordenamiento jurídico con la Ley 1042, tiene como fin proteger a las personas del nuevo espacio, llamado ciberespacio, que es una conexión entre redes de información dónde se desarrollan todo tipo de acciones virtuales, desde cualquier

²⁸ Real Academia Española. “*Diccionario panhispánico del español jurídico*” [en línea] [fecha de Consulta: el 8 de agosto de 2023]. Disponible en: <https://dpej.rae.es/lema/red-social>.

²⁹ Claro, Colombia. Loc. Cit.

³⁰ RODRÍGUEZ MADRIGAL, Bismarck, FLORES VASQUEZ, Fabio Ernesto, BERRIOS REYES, María Lissett. “*Los Delitos Informáticos y la Información como Nuevo Bien Jurídico Protegido*”. [en línea] León, junio 2006 [fecha de consulta: 06 de agosto 2023]. Disponible en: <http://riul.unanleon.edu.ni:8080/jspui/bitstream/123456789/1482/1/199275.pdf> P.9.

dispositivo que tenga conexión a internet, y que debido al mal uso o de una simple navegación en internet se puede afectar los bienes jurídicos de las personas de igual forma puede vulnerar a empresas e instituciones, públicas o privadas, en este espacio de latente peligro hacia intereses y usuarios que utilizan las TIC.

La responsabilidad del Estado es tutelar los derechos constitucionales, de los ciudadanos y según nuestra legislación estos delitos se enmarcan en el derecho público. Por tanto, es deber del Estado y como lo indica la misma ley 1042 en el art. 2 se declara de orden Público, por tanto, su persecución resulta de oficio.

1.5-Características de los Ciberdelitos.

Los ciberdelitos, agregan una nueva fase al Derecho Penal, y no cuentan con las características tradicionales de los delitos comunes. Adjuntan consigo características propias, y una problemática social relevante. Cuando hablamos de características propias de los ciberdelitos nos referimos, a su universalidad, extraterritorialidad, Instantaneidad y el ciberespacio.³¹

A)-Universalidad.

Debido al fenómeno global, el internet y su aceptación masiva, permite que en la mayoría de los hogares cuentan con los medios para acceder a las TICS. Es relevante mencionar que los componentes y los diseños con los que son fabricados los dispositivos actualmente acarrear una gran demanda, sobre todo al tener en común su ligereza, portabilidad, y fácil acceso.

Es esta demanda, la que abre un gran abanico de opciones a las personas en cuanto modelos, precios, especificaciones según las necesidades, y por ende la existencia de tantas opciones al alcance de la mano, amplía las posibilidades de cometer un ciberdelito o cualquier delito, desde cualquier parte del mundo, donde cualquier persona o sistema informático puede ser vulnerado sin importar la distancia, así los sujetos activos pueden estar en un país diferente de donde se comete el delito y los resultados pueden darse en

³¹ QUEZADA SALDAÑA, Martha Lorena. Loc. Cit. P.14.

un país distinto o lejano, igual se pueden dar simultáneamente en muchos países al mismo tiempo.

Por esta característica decimos que los ciberdelitos son universales, sobre todo por el fácil acceso para cualquier sujeto, en especial para el sujeto activo cuando se encuentra en otro país, y toma en cuenta que su ubicación este a un intervalo considerable del sujeto pasivo los hace creer inmune a la persecución por las autoridades y por ende no serán juzgado por cometer dichos delitos.

B)-Extraterritorialidad.

Esta característica, se debe a que estos delitos pueden ser cometidos y perseguidos tanto dentro del territorio Nacional, como Internacional, la persecución de estos delitos a nivel internacional se efectúa a través de los diversos convenios y acuerdos de cooperación de los Estados miembros, un ejemplo de estos sería El Convenio del Consejo Europeo o Convenio de Budapest, que fue adoptado en noviembre de 2001 y que entró en vigor en el 2004.³²

Este Convenio es el único que aborda, los ciberdelitos o cibercrimen; en su tercer capítulo determina sobre la cooperación internacional y establece disposiciones sobre asistencia mutua, en temas como acceso, conservación, obtención en tiempo real e interceptación de datos.

La cooperación entre Estados es necesaria por el hecho de que estos delitos, no son cometidos solo dentro del territorio nacional, sino que se extienden al territorio internacional por su efecto universal y para la debida persecución de quienes los cometen, es importante considerar que a medida que la tecnología avanza en igual medida avanza el índice de los ciberdelitos.

C)-Instantáneos

³² Vid. Convenio sobre la Ciberdelincuencia. Hecho en Budapest, el 23 de Noviembre del año 2001. Ratificado por Nicaragua Resolución 45/121 ONU (1990)

Esta característica se debe particularmente por su realización, es decir en su mayoría, son de consumación inmediata, pues pueden ocurrir en fracciones de minutos. Esta peculiaridad es más común en los ataques a sistemas informáticos de empresas, bancos o en algunos casos contra instituciones estatales, como ya se ha visto en diversos casos, al momento de perpetuar un ataque, ocurre en pocos minutos y pueden deshabilitar los sistemas de información por horas, tiempo suficiente para sustraer y filtrar gran cantidad de datos, incluso destruir software.

D)- Ciberespacio

Anteriormente hemos referido, que el ciberespacio se trata de un entorno complejo resultante de la interacción entre las personas, el software y los servicios en Internet por medio de dispositivos tecnológicos (TIC) conectados a redes.³³

Por lo que podemos decir que el ciberespacio es el lugar donde se efectúa la comisión de los ciberdelitos, esta una de las características más relevante, todo debido a que aporta un nuevo concepto dentro del derecho penal y que cambia tanto la práctica como la percepción en la forma que se cometen estos delitos.

Al tratarse de delitos muy técnicos, debido a que su ejecución se produce desde Dispositivos, o a través de redes, programas, ordenadores informáticos electrónicos además por el auge en una sociedad de crecimiento tecnológico a escala global, sumándole el fácil acceso al ciberespacio, facilita significativamente la comisión del ilícito, incluso para los niños, niñas y adolescentes siendo los más vulnerables y los más propensos de ser víctimas.

Cabe mencionar que, para la comisión de ciertos delitos, no es necesario que el sujeto activo cuente con un alto dominio de la informática y manejo de las Tecnologías de la Información y la Comunicación, aunque también para ciertos delitos si es necesario un conocimiento más amplio, sin embargo, en ambos casos, es significativo en la comisión

³³ Vid. Supra. p. 21.

del mismo el dolo, su premeditación, pues dependiendo el delito, el autor selecciona a su víctima, según el caso dado.

1.6. Clasificación de los Ciberdelitos

Los delitos reconocidos tienen una gran diversidad de infracciones, lo cual hace más difícil su clasificación o tipología, en cambio los ciberdelitos pueden clasificarse desde dos puntos de vista diferentes, dada la novedad de este fenómeno, el primero vendría siendo desde la doctrina con las ideas y principios que aportan los autores conocedores de la materia y la segunda es de acuerdo con la clasificación que le da la legislación.

Clasificación de los ciberdelitos Según Doctrina.

A disposición de Julio Téllez Valdez³⁴ y diversos autores expertos en la materia, los ciberdelitos se clasifican en base a dos criterios: como instrumento o medio, o como fin u objetivo.

- a) Como instrumento o medio: En esta categoría se encuentran aquellas conductas que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito.
- b) Como fin u objetivo: En esta categoría se encuadran las conductas dirigidas en contra de la computadora, accesorios o programas como entidad física.

Para María de la Luz Lima en su trabajo sobre "Delitos Electrónicos" los clasifica en tres categorías:

- a) Los que utilizan la tecnología electrónica como método (Conductas criminógenas en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito)
- b) Los que utilizan la tecnología electrónica como medio (Conductas criminógenas en donde para realizar un delito utilizan una computadora como medio o símbolo).

³⁴ VALDÉS, Julio Téllez. Ob. Cit. P.188.

- c) Los que utilizan la tecnología electrónica como fin (conductas criminógenas dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla).

Como método, los individuos utilizan métodos electrónicos para llegar a un resultado ilícito. Como medio, son aquellas conductas criminógenas en donde para realizar un delito utilizan una computadora como medio o símbolo. Y Como fin, son las dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla.³⁵

... “Otros autores como Quimbo clasifican los ciberdelitos en 3 tipos diferentes, según la víctima:

- a) Ciberdelitos contra las personas: transmisión de pornografía infantil o ciberacoso.
- b) Ciberdelitos contra la propiedad privada: acceso informático no autorizado, vandalismo informático, transmisión de programa maligno, posesión no autorizada de información digital, creación de virus o pirateo de software.
- c) Ciberdelitos contra la autoridad: ataques a webs del gobierno.

En esta línea, se propone una segunda tipología de delitos informáticos que establece diferencias entre aquellos que atentan directamente contra la intimidad, el honor o la propiedad privada de las personas físicas y aquellos que atentan contra las empresas, teniendo en cuenta que en ambos casos los métodos y objetivos pueden ser similares.”...

³⁶

Clasificación de lo ciberdelitos Según la Legislación.

³⁵ ECHEVARRIA ROMERO, Luis Miguel. “*Marco conceptual de los delitos informáticos.*” Maestría computación e informática, Universidad Mayor de San Marcos, Lima- Perú, 2005. P.22.

³⁶ FERNÁNDEZ FANJUL, María Luisa. “*Conceptualización, evolución y clasificación del ciberdelito empresarial. Definición del ciberdelincuente. Implicaciones estratégicas.*” Madrid: AMEC Ediciones, 2018. ISBN 978-84-946590-5-8. P. 70.

Uno de los sistemas de clasificación es el definido por el Convenio³⁷ sobre la Ciberdelincuencia, en el que se distinguen cuatro tipos diferentes de infracciones:

- a) Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos. - Sanciona el acceso y la interceptación ilegal, interferencia de datos y sistemas y el mal uso de dispositivos.
- b) Delitos de fraude informático. - Falsificación y fraude computacional.
- c) Delitos por su contenido. - Producción diseminación y posesión de pornografía infantil.
- d) Delitos relacionados con la infracción de la propiedad intelectual y derechos afines. - La amplia gama de reproducciones ilícitas por medios informáticos de obras protegidas por el derecho de autor.

Esta clasificación no es del todo coherente porque no se fundamenta en un criterio único para distinguir las categorías. De estas categorías, tres hacen referencia al objeto de la protección jurídica: “delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos; delitos relacionados con el contenido; y delitos relacionados con el derecho de autor”. La cuarta categoría, delitos informáticos, no se identifica con el objetivo de la protección jurídica sino con el método. Esta incongruencia hace que haya un poco de coincidencia entre las categorías.

... “La clasificación que el Estado de Nicaragua ha adoptado para clasificar los Ciberdelitos es la señalada por el Convenio de Budapest, y Naciones Unidas; doctrinariamente establecido por María de la Luz Lima

a) Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos y como método. -Capítulo II Delitos relacionados con la Integridad de los Sistemas Informáticos artos 4 al 11.

b) Delitos de fraude informático y como fin. - Falsificación y fraude computacional. Capítulo III, artos del 12 al 15 de la ley 1042.

³⁷ Vid. Convenio sobre la Ciberdelincuencia. Hecho en Budapest, el 23 de Noviembre del año 2001. Ratificado por Nicaragua Resolución 45/121 ONU (1990).

c) Delitos por su contenido y como medio. -Producción, diseminación y posesión de pornografía infantil. Capítulo IV, Delitos Relacionados con el Contenido de los Datos, artos.16 al 35 de la citada ley.”³⁸

1.7. Elementos teóricos básicos del Tipo Penal en los Ciberdelitos.

Conforme el crecimiento de las TIC, el verdadero reto para el Derecho Penal es ajustarse a las nuevas formas del ilícito penal, a causa del ciberespacio, como medio que genera la comunicación y que facilita en forma y recursos, cambiando así algunos aspectos fundamentales de lo que tradicionalmente asociamos como delito. Por ello, el Derecho debe ser más dinámico para posicionarse a la par de las problemáticas que van surgiendo conforme el avance tecnológico. Pese a que esto suene como un enunciado un poco pretencioso, debe tomarse en cuenta que la interacción entre sistemas conectados a la red está en constante cambio por el efecto de la globalización.

En el Derecho Penal, la ejecución de la conducta punible supone la existencia de dos sujetos, un sujeto activo y otro pasivo. Estos, a su vez, pueden ser una o varias personas naturales o jurídicas. De esta manera, el bien jurídico protegido será el elemento que defina a los sujetos y su posición frente al delito.

Según la teoría general del delito, los elementos del tipo penal se dividen en dos a saber, los elementos del tipo penal objetivo y del tipo penal subjetivo.

1.7.1- Tipo Penal Objetivo.

Los elementos objetivos del tipo penal son todos aquellos que caracterizan objetivamente la acción típica contenida en el supuesto de hecho de una norma penal, y están directamente relacionados a la realización material de la conducta y a la modificación de la realidad objetiva determinada por esta, generalmente los elementos objetivos son la acción típica, el sujeto activo, el sujeto pasivo, los elementos accesorios de modo, tiempo o lugar de realización de la acción típica, etc.

³⁸ QUEZADA SALDAÑA, Martha Lorena. Loc. Cit. P 18.

A)- Sujeto Activo

El sujeto activo es cualquier persona con la capacidad y el acceso, de cometer una o varias acciones, que como consecuencia causaren un mal, que constituya un delito contra el honor, la integridad, indemnidad, y libertad sexual de las personas; teniendo el suficiente dominio, o el básico de las tecnologías de información y comunicación, a través de los diversos dispositivos. Lo particular en estos delitos es que el sujeto activo no necesariamente tiene presencia física, pues realiza estas conductas ilícitas desde el plano digital, a través del ciberespacio.

Las personas que cometen este tipo de delitos son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, es decir que los sujetos activos tienen habilidades en el manejo de los sistemas informáticos y generalmente se encuentran en lugares estratégicos o se escudan bajo el anonimato y pueden entrar donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados.³⁹

B)-Sujeto Pasivo

El Sujeto pasivo es la persona física o moral sobre quien recae el daño o peligro causado por la conducta del delincuente. Por lo general, se le denomina también víctima u ofendido. En principio, cualquier persona puede ser sujeto pasivo; sin embargo, dadas las características de cada delito, en algunos casos el propio tipo penal señala quién puede serlo y en qué circunstancias. Por ejemplo, en los ciberdelitos solo puede ser sujetos pasivos todo aquello que hayan sido víctimas a través del uso de las TIC.

Los sujetos pasivos o victimas deben ser individuos que de la misma manera que el sujeto activo tiene acceso a las TIC; mediante el sujeto pasivo podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos.

³⁹ ACURIO DEL PINO, Santiago. “*Delitos Informáticos: Generalidades.*” [en línea] [fecha de Consulta: el 20 de agosto de 2023]. Disponible en: https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf P. 15.

C)- Acción típica.

En todo tipo hay una conducta, entendida como comportamiento humano (acción u omisión), que constituye el núcleo del tipo, es decir, su elemento más importante. La conducta viene descrita generalmente por un verbo rector («matar», «causar a otro una lesión», etc.), que puede indicar una acción positiva o una omisión. Cuando el tipo sólo exige la realización de la acción sin más, estamos ante los delitos de mera actividad (injuria, falso testimonio, etc.) o, en su caso, de mera inactividad (omisión pura, por ejemplo, omisión del deber de socorro). En otros casos se exige, junto a la realización de la acción, la producción de un resultado material de lesión o puesta en peligro de un bien jurídico.

D)- Bien Jurídico Tutelado.

El bien jurídico puede definirse como todo bien, situación o relación deseados y protegidos por el Derecho, constituyendo el eje central del orden social que el derecho penal protege.⁴⁰ El objeto jurídico es el bien lesionado o puesto en peligro por la conducta del sujeto activo. Jamás debe dejar de existir, ya que constituye la razón de ser del delito, y no suele estar expresamente señalado en los tipos penales.

Los bienes jurídicos protegidos en los ciberdelitos son algunos de los que se protegen en los delitos tradicionales, tales como el honor, y como lo expresa el capítulo la libertad e integridad sexual de las personas, estos delitos son casi el mismo fenómeno, pero con nuevas herramientas para delinquir, solo que agregando nuevo elemento como son las tecnologías de información y comunicación, lo que facilita la comisión, pero dificulta la persecución y sanción por parte del órgano jurisdiccional competente.

El Ciberespacio un nuevo bien jurídico emergente y necesario para proteger y regular, bienes inmateriales e intangibles como las redes, programas ordenadores, informática, confidencialidad e integridad de los datos, información, comunicación; bienes

⁴⁰ Palladino Pellón & Asociados Abogados Penalistas. “¿Qué protege el Derecho penal El bien jurídico en el Derecho Penal?” [en línea] [consultado el 20 de agosto de 2023]. Disponible en: <https://www.palladinopellonabogados.com/el-bien-juridico-en-el-derecho-penal/>

patrimoniales, Libertad sexual, Honor e intimidad de las personas, bienes corporativos, Seguridad de la Nación.

Podemos decir que el bien jurídico protegido en general es la información, pero está considerada en diferentes formas, ya sea como un valor económico, como un valor intrínseco de la persona, por su fluidez y tráfico jurídico, y, por último, por los sistemas que la procesan o automatizan; los mismos que se equiparan a los bienes jurídicos protegidos tradicionales.

E)- Elementos Accesorios.

Los elementos accesorios de comisión del delito se refieren al modo o forma, al tiempo y al lugar de comisión del hecho, en el caso de los ciberdelitos estos son cometidos de forma virtual o digital, en cualquier tiempo y en el ciberespacio, entendiéndose este último como una realidad virtual.

1.7.2- Tipo Penal subjetivo.

Existen algunas conductas que, para ser relevantes para el Derecho penal, han de poseer alguna finalidad o intencionalidad específica. De suerte que, si no contienen ese especial ánimo del sujeto, no interesan y no comportan el significado necesario para crear un riesgo o para dañar el bien jurídico protegido. Por consiguiente, el legislador, al describir estas conductas en la norma, lo hace mencionando expresamente la referencia anímica, intencional o finalista, sin la cual la conducta es absolutamente irrelevante. En definitiva, estas referencias al ánimo, a la intención o a la finalidad con la que actuó el sujeto, pertenecen al tipo, pues sin ellas el comportamiento no significa nada para el Derecho penal. De ahí que a este conjunto de referencias subjetivas intencionales o anímicas se les llame “elementos subjetivos del tipo”⁴¹.

A)- Elemento subjetivo de autoría.

⁴¹ ORTS BERENGUER, Enrique y GONZÁLEZ CUSSAC, José, “**Manual de Derecho Penal. Parte General**”, proyecto de reforma y modernización normativa, CAJ/FIU-USAID, Managua, 2004. p.83.

En algunos casos la ley exige determinadas cualidades para ser sujeto activo de un delito. Nos encontramos entonces con los llamados delitos especiales.

El autor de estos delitos sólo puede serlo aquella persona que, además de realizar la acción típica, tenga las cualidades exigidas en el tipo, por ejemplo, ser socio o accionista en una sociedad mercantil para poder cometer un delito societario; ser juez o magistrado para poder cometer un delito de prevaricato; ser funcionario público para poder cometer un delito de malversación de caudales públicos, etc.

Estos delitos plantean especiales dificultades en relación con el tratamiento que debe darse a aquellos partícipes que intervienen en la realización del delito especial sin tener las cualidades personales exigidas en el tipo

En el caso de los ciberdelitos aquí abordados el elemento subjetivo de autoría básica que vemos en ellos es ser mayor de edad, sin embargo, podemos observar las agravantes que plantea al artículo 35 de la ley 1042, en este caso cuando los sujetos activos son familiares, funcionarios públicos, tutores o Toda persona que prevaliéndose de la superioridad originada por relaciones de confianza, educativa, de trabajo o cualquier otra relación, pero aclarando que estas condiciones las contempla la ley como agravantes, pero no como condición sine qua non del elemento subjetivo de autoría del tipo básico.

B)- Dolo.

El Dolo consiste en causar intencionalmente el resultado típico, con conocimiento y conciencia de la antijuricidad del hecho.⁴² Obra con dolo quien quiere la realización del hecho tipificado (elemento volitivo), así como quien la acepta (elemento cognitivo o intelectual), previéndola a lo menos como posible.

En el caso de los ciberdelitos contra la integridad, indemnidad y libertad sexual son dolosos únicamente.

⁴² DE LA CUESTA AGUADO, Paz, *Tipicidad e Imputación Objetiva*, extracto del artículo publicado en La imputación objetiva en el Derecho penal de Claus ROXIN, Editorial IDEMSA, Lima (Perú) 1997.

C)- Imprudencia.

Mientras las conductas dolosas consisten en que la acción es emprendida con la finalidad de realizar la lesión al bien jurídico, la conducta imprudente es la acción peligrosa emprendida sin ánimo de lesionar el bien jurídico, pero, que por falta de cuidado o negligencia debida, causa su efectiva lesión.⁴³

Es un tipo estructuralmente propio y distinto del doloso, cuyo injusto está constituido objetivamente por la producción del resultado típico, consecuencia de una acción que infringe el deber normativo de cuidado y en lo subjetivo por la capacidad individual de prever efectivamente el peligro de realización del resultado típico.

Actúa con imprudencia quien cause un resultado no querido, pero previsible y evitable, como consecuencia directa de la infracción a un deber de cuidado.

En el caso de los ciberdelitos contra la integridad, indemnidad y libertad sexual no existe la comisión por imprudencia.

⁴³ MUÑOZ CONDE, Francisco y GARCÍA ARAN, Mercedes, *Derecho Penal: Parte General*, 7ma Edición, Bogotá, Colombia, Ed. Tirant Lo Blanch, 2010.

CAPÍTULO II. CIBERDELITOS CONTRA LA INTEGRIDAD, INDEMNIDAD Y LIBERTAD SEXUAL.

En este estudio nos referiremos específicamente a los Ciberdelitos cometidos contra la integridad y libertad sexual, como nuevo fenómeno recientemente integrado al Derecho Penal, y por tratarse de delitos de contenido, afectan la imagen e integridad de las personas.

Cabe destacar que dentro de este artículo incluimos un término que no está dentro de la Ley, y es la “indemnidad”; término utilizado para la protección de los y las menores y que debería ser incluido, por ser mucho más vulnerables y potenciales víctimas, es de conocimiento público que muchos, niños, niñas o adolescentes comienzan a utilizar dispositivos conectados a las redes de información desde temprana edad, llámeseles redes sociales, mensajería de texto, o cualquier medio con el que puedan comunicarse, convirtiéndolos en objetivos vulnerables.

La Ley 1042 para poder abordar esta nueva modalidad de delitos a través de las TIC integran puntos muy básicos, pero no muy específicos sobre las características de los ciberdelitos que pueden afectar los bienes jurídicos tutelados de las personas y las más vulnerables, así mismo la Ley no integra varios tipos de delitos referidos a la integridad sexual, que en la realidad social son cometidos, pero no perseguidos por el hecho de no estar tipificados. Por tanto, es meritorio en esta investigación dedicar un capítulo dividido en dos acápite. El primero abarca los delitos tipificados y establecidos en la legislación vigente y el segundo sobre todos aquellos ciberdelitos que no es tan tipificados, pero aun así están presente dentro de la realidad nicaragüense y que radica problemas a la realidad social de nuestro país.

2.1. TIPOS DELICTIVOS TIPIFICADOS EN LA LEGISLACIÓN NACIONAL.

Una de las características que diferencian estos delitos de los comunes es que estos se mantienen a perpetuidad en las redes, es decir a pesar de haber borrado la fuente de origen, si este se compartió, los datos aun existirán dentro de la redes de información, y destaca que la mayoría de los delincuentes que cometen estos delitos se esconden en

el anonimato pero debido a los diferentes tipos de medios que crean las TIC se pueden conservar datos, y esto puede servir para la búsqueda del origen del posible culpable.

2.1.1-Utilización de niñas, niños, adolescentes o personas con discapacidad necesitada de especial protección, en pornografía a través del uso de las Tecnologías de la Información y la Comunicación⁴⁴.

Como en toda sociedad los y las menores de edad resultan ser los más vulnerables y potenciales víctimas de gran variedad de delitos, con el avance de las TICS al ser un medio para la difusión de esta clase de materiales, donde usuarios de todo el mundo pueden compartir cualquier tipo de archivos, solo favorecen a que el fenómeno delictivo de la pornografía infantil vaya al alza. Estas nuevas tecnologías han creado un entorno que no solo facilita el acceso, si no que aumenta la producción y distribución de la pornografía infantil.

Al considerar el peligro en que se encuentran los menores por las TIC los legisladores de nuestro país y bajo la influencia de los diversos tratados internacionales como el Convenio de la niñez y adolescencia, el tratado de Budapest, debido a estos, se incluyen dentro de la ley 1042 en el Artículo 31 la utilización de niñas, niños, adolescentes o personas con discapacidad necesitadas de especial protección, en pornografía a través del uso de las Tecnologías de la Información y la Comunicación. En referencia a que no solo se debe proteger a los menores, sino que la Ley también protege a todas las personas que necesitan una protección especial, considerando el caso dado, de ser utilizadas en actividades de este tipo, siendo que presenten limitaciones temporales o permanentes, en sus capacidades sensoriales, físicas o intelectuales.

El artículo 31 expresa las diferentes características bajo las que actúan los posibles criminales, primeramente, expresa que, para ser juzgado procesalmente bajo este delito, el delincuente o posible acusado debe actuar por medio de las tecnologías de la información y comunicación, en pocas palabras este debe utilizar cualquier dispositivo que esté conectado con el ciberespacio. Nos habla sobre las conductas que debe

⁴⁴ Arto. 31. Ley 1042, Ley Especial de Ciberdelitos, en La Gaceta, Diario Oficial N°. 201 de 30 de octubre de 2020.

cumplirse para poder efectuarse como delito, expresa que quien induzca, facilite, promueva, utilice, abuse o explote con fines sexuales o eróticos haciéndola presenciar o participar en un comportamiento, espectáculo o acto sexual público o privado, no especifica de qué manera pueden ser las actuaciones de parte del autor del delito, para efectuarlo, no habla de los medios en que se podrían cometer y tampoco habla de cómo el autor del delito puede acercarse a sus víctimas.

Dejando en evidencia un vacío, al no estar muy claro y no expresar que pasa en los casos de las personas que hagan distribución y manejo de material sin necesidad de interactuar directamente con los menores, así mismo no expresa si las personas que son consumidoras de este tipo de material podrán ser penalmente punibles, porque a pesar de no cometer acciones directamente contra menores consumen este tipo de material y se vuelven propensos a ser posibles actores de estos delitos, poniendo en peligro a los menores.

La libertad e integridad sexual, o bien, la indemnidad sexual para las personas menores de edad es el bien jurídico que se tutela en el capítulo V de la Ley 1042, por ende, consideramos que debe definir preceptos más claros al momento de establecer las actuaciones que deben realizarse para poder encuadrar cualquier conducta delictiva dentro esta modalidad criminal, y continuar así su persecución penal.

Es importante aclarar que el término “pornografía infantil” no está tipificado con ese nombre en nuestra legislación, ni en esta ley de ciberdelitos ni en el código penal, utilizándose términos sustitutos como pornografía con menores de edad o con niños, niñas u adolescentes, sin embargo la pornografía infantil, cobra grandes y graves dimensiones, a través de la Internet, porque en su mayoría los criminales escudados bajo ese perfil anónimo pueden estar en contacto simultáneamente con otras personas desde otro sitio del planeta, hace posible que las imágenes o representaciones de naturaleza pornográfica sean conocidas o distribuidas de inmediato, unido esto a la existencia de otras lesiones que hacen irreparable la violación a los derechos de las víctimas.

Situación que además se agudiza desde el punto de vista procesal, dado el problema investigativo que de esto deriva y de la impunidad que se genera respecto de aquellos que se encuentran fuera del territorio nacional.

La pornografía infantil representa sin duda uno de los fenómenos criminales más preocupantes, su expansión se ve especialmente favorecida por las capacidades del Internet y la globalización en las comunicaciones. En consecuencia, constituye uno de los sectores prevalentes donde con mayor intensidad se ha centrado el esfuerzo de la cooperación penal internacional, y que se ha plasmado no sólo con la celebración en 2001 del señalado Convenio sobre la Ciberdelincuencia en Budapest, sino también en la actuación conjunta y coordinada de las Fuerzas y Cuerpos de Seguridad en numerosos operativos en distintos países del mundo.⁴⁵

Artículo. 31. Utilización de niñas, niños, adolescentes o personas con discapacidad necesitada de especial protección, en pornografía a través del uso de las Tecnologías de la Información y la Comunicación.

Quien, por medio del uso de las Tecnologías de la Información y la Comunicación, induzca, facilite, promueva, utilice, abuse o explote con fines sexuales o eróticos a niñas, niños, adolescentes o personas con discapacidad necesitada de especial protección, haciéndola presenciar o participar en un comportamiento, espectáculo o acto sexual público o privado, se le impondrá pena de cinco a ocho años de prisión y trescientos a seiscientos días multa.

No se reconoce, en ninguno de los supuestos descritos en el párrafo anterior, valor al consentimiento de la víctima.

Sujeto activo: es indeterminado.

⁴⁵ ANDRES BARRIOS, Moisés. *“Delitos 2.0: aspectos penales, procesales y de seguridad de los ciberdelitos”*. [en línea] 1ª ed. Madrid: Wolters Kluwer España, 2018. [fecha de consulta: 25 de agosto del 2023]. ISBN 978-84-9020-744-4. Disponible en: [E Libro](#) .

Sujeto pasivo: en este caso es determinado: niñas, niños, adolescentes o personas con discapacidad necesitada de especial protección

Acción típica: inducir, facilitar, promover, utilizar, abusar o explotar con fines sexuales o eróticos a niñas, niños, adolescentes o personas con discapacidad necesitada de especial protección, haciéndola presenciar o participar en un comportamiento, espectáculo o acto sexual público o privado.

Elementos accesorios: en este caso son de modo o forma: “por medio del uso de las Tecnologías de la Información y la Comunicación”

Elementos normativos: “Tecnologías de la Información y la Comunicación” , “fines sexuales o eróticos”, “personas con discapacidad necesitada de especial protección”, “espectáculo o acto sexual”.

Dolo: este tipo penal es de comisión dolosa únicamente.

2.1.2- Corrupción a personas menores de 16 años o personas con discapacidad necesitada de especial protección a través del uso de las Tecnologías de la Información y la Comunicación.⁴⁶

La facilidad de la comunicación junto al acceso a diferentes culturas ha permitido la aparición de nuevas tipologías delictivas, o modernización de las ya existentes relacionadas. Una de las razones de esta problemática es que algunos padres a fin de compensar a modo de ocupaciones para sus hijos les entregan de forma libre dispositivos conectados a internet, muchas veces esta acción parece inofensiva y le restan atención a sus hijos sobre con quienes interactúan en la red, sin prever los diversos riesgos.

Esta es una problemática latente, donde los niños, niñas y adolescentes pueden ser potenciales víctimas con los comunes *modus operandi* de los victimarios que desean satisfacer sus depravados deseos sexuales, ante esta situación. La Ley 1042 hace

⁴⁶ Arto. 32. Ley 1042, Ley Especial de Ciberdelitos, en La Gaceta, Diario Oficial N°. 201 de 30 de octubre de 2020.

referencia en el artículo 32 sobre la corrupción a personas menores de 16 años o personas con discapacidad necesitada de especial protección a través del uso de las TIC.

Es fundamental hacer la distinción de este delito con el de pornografía con menores de edad, por el hecho que en este delito el actor es toda persona mayor, el cual hace propuestas, decir propone realizar actos o encuentros de carácter sexual o eróticos con menores, ganando su confianza, convenciéndolo a través de las redes o así mismo prometiéndoles algo a cambio, es decir el autor busca el consentimiento de la víctima para realizar los encuentros o producir pornografía, pero nuestra legislación establece que el consentimiento de la responsabilidad jurídicas del menor no exime de la responsabilidad del adulto.

Este delito no fue abarcado de una forma completa por el legislador ya que solo habla de propuestas, de supuesto de acción en la que personas mayores proponen a menores actos de carácter sexual o erótico y no habla de la consumación del delito que de qué manera se va a actuar en caso de efectuar el acto con el menor, es decir por ejemplo si el victimario obtuvo el consentimiento de la víctima valiéndose de engaños y dicho acto carnal es consumado y transmitido a través de las TICS.

Artículo 32 Corrupción a personas menores de 16 años o personas con discapacidad necesitada de especial protección a través del uso de las Tecnologías de la Información y la Comunicación

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 para sostener encuentros de carácter sexual o erótico, o para la producción de pornografía a través del uso de las Tecnologías de la Información y la Comunicación para sí o para terceros, se le impondrá pena de uno a tres años de prisión.

Sujeto activo: es indeterminado.

Sujeto pasivo: en este caso es determinado: personas menores de 16 años o personas con discapacidad necesitada de especial protección.

Acción típica: hacer propuestas implícitas o explícitas para sostener encuentros de carácter sexual o erótico, o para la producción de pornografía

Elementos accesorios: en este caso son de modo o forma: “por medio del uso de las Tecnologías de la Información y la Comunicación”.

Elementos normativos: “propuestas implícitas o explícitas”, “personas con discapacidad necesitada de especial protección”, “carácter sexual o erótico”, “pornografía” y “Tecnologías de la Información y la Comunicación”.

Dolo: este tipo penal es de comisión dolosa únicamente.

2.1.3- Acoso a través del uso de las Tecnologías de la Información y la Comunicación⁴⁷

Bajo este fenómeno jurídico, el acosador tiene como propósito vigilar los movimientos diarios de la víctima a través de las redes sociales, Facebook, Instagram, Twitter y una vez obtenida la información privada comienza a crear hábitos iniciando conversaciones con la víctima, creando lazos de comunicación y en un momento dado incitaciones de índole sexual, u obsesión amorosa, esta situación lleva a la víctima a encontrarse en peligro no solo por el uso de su información, si no también físicamente porque el acosador al tener sus datos, gracias a esto sabe cómo localizarla y poder actuar en contra de la posible víctima.

Sin embargo, en el actuar criminal a través de las TIC es denominado, socialmente como “Ciberacoso” y según el Departamento de Salud y Servicios Humanos de los Estados Unidos ... “El ciberacoso es el acoso que tiene lugar en dispositivos digitales, como teléfonos celulares, computadoras y tabletas. El ciberacoso puede ocurrir mediante mensajes de texto, textos y aplicaciones, o bien por Internet en las redes sociales, foros o juegos donde las personas pueden ver, participar o compartir contenido. El ciberacoso incluye enviar, publicar o compartir contenido negativo, perjudicial, falso, o cruel sobre otra persona. Esto puede incluir compartir información personal o privada sobre alguien

⁴⁷ Arto. 33. Ley 1042, Ley Especial de Ciberdelitos, en La Gaceta, Diario Oficial N°. 201 de 30 de octubre de 2020.

más, provocándole humillación o vergüenza. Algunos acosos por Internet pasan a ser un comportamiento ilegal o criminal.

Los lugares más comunes donde ocurre el ciberacoso son:

- Redes sociales, como Facebook, Instagram, Snapchat y Tik Tok
- Mensajes de texto y aplicaciones de mensajería en dispositivos móviles y tabletas
- Mensajería instantánea, mensajes directos y chats por Internet
- Foros en Internet, salas de chat y tableros de mensajes, como Reddit
- email
- Comunidades de juegos en Internet” ... ⁴⁸

El ciberacoso es un comportamiento agresivo y no deseado para el que lo recibe, entre niños, niñas y adolescentes, también puede ser entre adultos, este involucra un desequilibrio de poder real o percibido. El comportamiento se repite o tiende a repetirse con el tiempo. Tanto los que son acosados como los que acosan pueden padecer problemas graves y duraderos.

Este delito, bajo esta modalidad criminal de igual forma debe ser analizado por nuestra legislación ya que con anterioridad solo se regulaba el acoso sexual y no se tomaba el acoso común como un delito, pero debido al crecimiento de los medios y la problemática social en el que muchos niños, niñas y adolescentes se han visto afectados hasta el punto de llegar a necesitar ayuda psicológica por la constante humillación a la que se sienten sometidos. Atendiendo lo precitado, tipifica las acciones necesarias con las que debe cumplir el victimario y que las exterioriza final y directamente hacia la víctima afectando su estabilidad psicológica y emocional.

⁴⁸ Stopbullying.gov. “*Que es el ciberacoso.*” [en línea] [fecha de consulta: 16 de agosto del 2023]. Disponible en: <https://espanol.stopbullying.gov/acoso-por-internet-1yqc/qu%C3%A9-es>.

Artículo 33 de la Ley 1042. Acoso a través del uso de las Tecnología de la información y la comunicación.

Quien atormente, hostigue, humille, insulte, denigre u otro tipo de conducta que afecte la estabilidad psicológica o emocional, ponga en riesgo la vida o la integridad física por medio del uso de las Tecnologías de la Información y la Comunicación.

Cuando la víctima sea niña, niño, adolescente o persona con discapacidad necesitada de especial protección, se impondrá pena de cuatro a seis años de prisión.

Sujeto activo: es indeterminado.

Sujeto pasivo: en el primer párrafo del tipo es indeterminado, sin embargo, en el segundo párrafo es determinado: niña, niño, adolescente o personas con discapacidad necesitada de especial protección.

Acción típica: atormentar, hostigar, humillar, insultar, denigrar u otro tipo de conducta que afecte la estabilidad psicológica o emocional, ponga en riesgo la vida o la integridad física

Elementos accesorios: en este caso son de modo o forma: “por medio del uso de las Tecnologías de la Información y la Comunicación”.

Elementos normativos: “atormentar”, “hostigar”, “humillar”, “insultar”, “denigrar”, “estabilidad psicológica o emocional”, “riesgo”, “vida”, “integridad física”, “personas con discapacidad necesitada de especial protección” y “Tecnologías de la Información y la Comunicación”.

Dolo: este tipo penal es de comisión dolosa únicamente.

2.1.4. Acoso sexual a través del uso de las Tecnologías de la Información y la Comunicación.⁴⁹

El acoso sexual es cualquier insinuación sexual no deseada, solicitud de favor sexual, conducta verbal o física o gesto de naturaleza sexual, o cualquier otro comportamiento

⁴⁹

de naturaleza sexual que razonablemente se pueda esperar o se pueda percibir que causa ofensa o humillación a otra persona. El acoso sexual puede ocurrir entre personas del mismo sexo o del sexo opuesto. Tanto hombres como mujeres pueden ser víctimas o delincuentes.⁵⁰

El acoso sexual incluye formas sin contacto físico, como comentarios sexuales sobre partes del cuerpo o la apariencia de una persona, silbidos, peticiones de favores sexuales, miradas sexualmente sugerentes, acecho, y la exposición de los órganos sexuales de una persona a otra, con el avance de las TIC esto pasa a convertirse en algo digital porque ahora se realiza a través de mensajes, imágenes, videos todos estos de contenido sexual, dando insinuaciones que infundan y crean miedo a la víctima.

Esta acción puede perjudicar a personas de ambos sexos. En muchos países es considerado un acto delictivo y sancionado conforme su gravedad y que puede llevar incluso a la privación de libertad del acosador. Bajo esta modalidad realizada a través del ciberespacio.

Con la tipificación de este delito en el artículo 34 de la ley 1042, este tipo penal tiene un cambio significativo y actual debido a que, anterior a la Ley ya mencionada dicha acción penal se mantenía bajo un plano físico cuando cualquier persona realizaba actos lascivos o lúbricos tocamientos en otra persona, sin su consentimiento, esto según el código penal en su artículo 172 son los caso donde existe acoso sexual, y la Ley especial viene a cambiar el modo en que opera el delito de acoso sexual ya que la característica en donde era necesario el contacto desaparece y es reemplazada por toda acción que puede realizar cualquier persona mayor de edad, enviando mensajes, frases, fotografías, vídeos u otra acción inequívoca de naturaleza o contenido sexual a otra persona sin su consentimiento.

Esto pasa a ser un asecho en el plano digital en donde no se necesita la presencia física de acosador, estos pueden interactuar con las victimas al estar conectados a través del

⁵⁰ ONU Women. “Prohibición de la discriminación, el acoso, incluido el acoso sexual, y el abuso de la autoridad” [en línea] [fecha de consulta: el 25 de agosto de 2023]. Disponible en: <https://www.un.org/womenwatch/uncoordination/antiharassment.html>

internet en aplicaciones de mensajerías y esto les da la posibilidad de interactuar a través de dispositivos y muchos kilómetros del domicilio de la víctima hasta poder encontrarse fuera del país, este factor junto con el anonimato hace que este delito se vuelva más difícil al momento de su persecución.

Artículo 34 Acoso sexual a través del uso de las Tecnologías de la Información y la Comunicación.

Cuando una persona mayor de edad envíe mensajes, frases, fotografías, videos u otra acción inequívoca de naturaleza o contenido sexual a otra persona sin su consentimiento a través del uso de las tecnologías de la información y la comunicación se le impondrá pena de dos a cuatro años de prisión.

Cuando la víctima sea menor de 16 años, con o sin su consentimiento o persona con discapacidad necesitada de especial protección se le impondrá pena de cuatro a seis años de prisión.

Sujeto activo: está determinado a ser mayor de edad.

Sujeto pasivo: en el primer párrafo del tipo es indeterminado, sin embargo, en el segundo párrafo es determinado: menor de 16 años o personas con discapacidad necesitada de especial protección.

Acción típica: enviar mensajes, frases, fotografías, videos u otra acción inequívoca de naturaleza o contenido sexual a otra persona sin su consentimiento.

Elementos accesorios: en este caso son de modo o forma: “por medio del uso de las Tecnologías de la Información y la Comunicación”.

Elementos normativos: “ mensajes”, “frases”, “fotografías”, “vídeos”, “contenido sexual”, “personas con discapacidad necesitada de especial protección” y “Tecnologías de la Información y la Comunicación”.

Dolo: este tipo penal es de comisión dolosa únicamente.

2.2. TIPOS DELICTIVOS CALIFICADOS COMO CIBERDELITOS NO TIPIFICADOS EN LA LEGISLACIÓN NACIONAL.

Desde el surgimiento de las tecnologías de comunicación hasta el desarrollo de dispositivos como teléfonos, tabletas, computadoras, han surgido peligros a partir de su uso, cuyo riesgo alcanza tanto a niños, niñas, como adolescentes. Actualmente se cometen muchas acciones delictivas que no están tipificadas y no son reflejadas en nuestra legislación, que directamente afectan los derechos de las demás personas y que el legislador no tomó en cuenta al momento de crear la ley 1042 bajo la realidad social, acciones que ocurren a través de las nuevas tecnologías que van creciendo al mismo ritmo que la sociedad, muchas de estas son perseguidas como delitos comunes, pero aun así muchas de las acciones cometida no caben dentro las características típicas de los delitos penales comunes que ya están en nuestro ordenamiento Legal.

1.1. Cyberbullying.

El Cyberbullying es una adaptación de las palabras en inglés cyber y bullying; en español lo conocemos como ciber abuso o violencia entre iguales. *Cyberbullying* es un término que se utiliza para describir cuando un niño o adolescente, es molestado, amenazado, acosado, humillado, avergonzado o abusado por otro niño o adolescente, a través de Internet o cualquier medio de comunicación como teléfonos móviles o tables.⁵¹

Este es un término que se ha vuelto muy común dentro de nuestra sociedad, se podría decir que el cyberbullying es un problema de la era digital ya que este nace junto con las tecnologías de información y comunicación, es cometido en gran cantidad a través de dispositivos conectados a las TIC, pero no existe alguna regulación específica en nuestra legislación y muchas veces es tratado como acoso, pero, aunque son parecidos este tiene una característica que lo diferencia.

El cyberbullying es el uso de las nuevas tecnologías de la información (principalmente Internet, telefonía móvil y videojuegos online) para ejercer el acoso psicológico entre

⁵¹ CORONA, Pablo. “¿Qué es el cyberbullying?” [en línea] [fecha de consulta: 01 de septiembre de 2023]. Disponible en: <https://www.gob.mx/cyberbullying/articulos/que-es-el-cyberbullying>.

iguales. Es el hostigamiento a través de medios informáticos como redes sociales, chat, correo electrónico o sitios web. Consiste en molestar, amenazar, humillar o acosar a una persona utilizando dichos medios.

Las formas más comunes son la difusión de falsos rumores, videos o fotos humillantes, y la creación de perfiles o sitios para agredir a la víctima. También puede ocurrir que el agresor se haga pasar por otra persona para decir cosas desagradables o amenace a la víctima con publicar su información personal. Generalmente, los afectados son personas vulnerables que son vistas como “diferentes” por quien las molesta.

El cyberbullying se expande viralmente por la Web y puede ser difícil de detener, Por tal motivo, resulta invasivo y dañino. Además, puede que las agresiones permanezcan en el ciberespacio durante mucho tiempo, por lo que afectan a largo plazo a quien las sufre.⁵²

Uno de los mayores inconvenientes que se presenta en el Cyberbullying es que los agresores que utilizan las redes para insultar o burlarse de la víctima, también difunden rumores e incluso mentiras, y se protegen casi siempre en el anonimato; a diferencia del hostigamiento tradicional, que habitualmente consiste en la confrontación cara a cara, las víctimas cibernéticas no pueden ver o identificar a sus acosadores, lo que los hace sentir aún más indefensos y vulnerables. El anonimato es uno de los factores que perpetúa, en este tipo de prácticas.

La conducta típica del acosador suele responder a las siguientes características: es intencional, persistente y agresiva. Podemos señalar un elemento característico “la intención de daño”, es decir, la evidencia de que existe un definido propósito de perjudicar a la víctima. Un aspecto que lo diferencia del acoso es el hecho que, en el acoso, el agresor busca hacer daño directamente a la víctima, es decir afectarla en su vida diaria y personal, mientras que en el Cyberbullying; el agresor busca perjudicar a la víctima de

⁵² Argentina Cibersegura. “*Ciberbullying ¿Qué es?*” [en línea] [fecha de consulta: 6 de septiembre de 2023]. Disponible en: https://www.argentinacibersegura.org/admin/resources/files/consejos/31/Guia_sobre_Cyberbullying.pdf

manera pública, ya no solo afecta su integridad y estabilidad psicológica, sino que afecta su imagen y honor en las redes o cualquier medio de comunicación.

Existen muchos casos en el que personas han sido víctima de Cyberbullying en las redes sociales, dañando su integridad, creando memes y difundiéndolos, afectando la integridad en la víctima, consecuentemente enfermándose psicológica y emocionalmente, pueden padecer crisis depresivas, empezar a ensimismarse en si mismos y construyendo un muro como mecanismo de protección entre ellos y el mundo en muchas ocasiones, debido al grado de humillación que sufren en las redes, hasta en los peores casos el suicidio.

2.3. Sexting.

Se denomina sexting a la actividad de enviar fotos, videos o mensajes de contenido sexual y erótico personal a través de dispositivos tecnológicos, ya sea utilizando aplicaciones de mensajería instantánea, redes sociales, correo electrónico u otra herramienta de comunicación. La palabra sextina es un acrónimo en inglés formado por 'sex' (sexo) y 'texting' (escribir mensajes)⁵³

Con el avance de las tecnologías, los adolescentes y adultos joven ocupan la mayoría del tiempo en el uso del internet, ya sea a través de la computadora o en sus dispositivos móviles, actualmente es común que la mayoría de sus actividades las dediquen a utilizar las redes sociales, conocer personas, jugar online o ver videos, pero en los últimos años una nueva moda ha causado polémica, se trata de mandar mensajes con imágenes y textos con carácter sexual, esta moda es llamada por los jóvenes "pásame tu pack", esta frase es muy escuchada en las secundarias y universidades, cuando una persona manda el pack a la persona incorrecta este se viraliza y se vuelve de dominio público, esta acción dentro de los jóvenes puede parecer divertida y sin consecuencias pero en realidad no lo es, porque, difundir una imagen o fotografía de alguien desnudo o semidesnudo es una acción que se identifica como sexting y que puede causar mucho daño a la persona que es víctima de esto, siendo objeto de burlas, criticas, y causar cierto daño

⁵³ IntraMed. *¿Qué es el sexting?* [en línea] [consultado el 06 de septiembre de 2023]. Disponible en: <https://www.intramed.net/contenidoover.asp?contenido=93210>.

psicológicamente como física, por eso esta razón debería considerarse como un delito especial, ya que la modalidad de este no se adecua a las conductas comunes que conocemos.

Usualmente el sexting se da en relaciones de pareja o parejas ocasionales, pero siempre existiendo un elevado grado de confianza entre las partes, o cuando se realiza el envío de dicho material para que sea visto involuntariamente por el receptor. En este último supuesto tenemos tres variantes, de las cuales una de ellas, de momento, es atípica y se da cuando el emisor y el receptor son personas mayores de 18 años.⁵⁴

Esta actividad lesiona la intimidad, el honor y al derecho a la propia imagen de la víctima, el derecho a la imagen integra el derecho a la privacidad protegido por el artículo 26 de la Constitución.

El fácil acceso a las TIC hace que esta acción se haga más común entre jóvenes, en esta acción existe un mutuo acuerdo, entre dos personas, pero una de esas personas abusando de la confianza que se le ha dado este las comparte y se hacen de dominio público, pudiendo repercutir en daños en la imagen pública de la persona que es víctima, lo que conlleva a problemas en relaciones interpersonales con padres, amigos y en algunos caso con problemas laborales al dañar la imagen de dicha persona, problemas psicológicos , emocionales y hasta llevar a la depresión esta acción no es reflejada en la legislación debería ser considerada como un delito doloso que se trate de una figura penal la cual debe pretender tutelar la libertad de las personas referida al contenido de las comunicaciones privadas que pertenece a la esfera de la reserva del comunicador y solo debe ser conocida por el sujeto a quien va dirigida.

⁵⁴ ALVAREZ, Teodoro Javier. *“Delitos Sexuales Coerción sexual e internet Grooming- Sexting- Sextortion-Stalking”*. 1ª ed. Buenos Aires: Ediciones DyD, 2018. ISSN: 978-987-9371-85-5. P. 23

2.4. Sextorsión.

Sextorsión es una amenaza de diseminación de imágenes explícitas, íntimas o embarazosas de naturaleza sexual sin consentimiento. Usualmente es con el propósito de obtener más imágenes, actos sexuales, dinero u otra cosa.⁵⁵

El mismo consiste en la amenaza, chantaje o extorsión sexual que se le hace a una persona, previamente filmada o fotografiada desnuda o realizando actos sexuales en la intimidad, a cambio de dinero para no publicar las imágenes o videos. También para exigirle que entregue más fotografías de ella o de otra persona. Otra variante es que sea obligada a mantener relaciones sexuales. La conducta típica que existe en este delito es la que el agresor, al tener material de la víctima, lo utiliza como un elemento de control sobre la víctima.

Aquí, puede o no existir una relación previa, las fotografías o material pornográfico pueden ser obtenidas por medio de otra persona (quien si tenía una relación con la víctima y divulgo el material), extraídas de alguna red o como consecuencia de un encuentro sexual ocasional. El sujeto activo lo que persigue es la obtención de dinero o favores sexuales tanto para el como para un tercero por medio de la extorsión.

En Nicaragua esta conducta no está tipificada, pero sí está regulada la extorsión en el artículo 228 del Código Penal, de cualquier manera, se considera importante incluirlo en un apartado diferente ya que aquí se encuentra comprometida la intimidad y la integridad sexual de la víctima, lo que diferencia a la sextorsión de la extorsión común, es que en este caso, no solo compromete la voluntad y el patrimonio de la víctima también pone en peligro su sexualidad y puede llegar hasta el punto de inicio hacia otro delito tal como violación entre otros casos en los cuales violentaría sus derechos de carácter sexual, tenemos que tener en cuenta que este es delito solo puede cometerse de manera dolosa.

⁵⁵ IntraMed. *¿Qué es la "sextorsion"? Estudio sobre la amenaza cibernética de más rápido crecimiento en adolescentes en los Estados Unidos* [en línea] [consultado el 07 septiembre de 2023]. Disponible en: <https://www.intramed.net/contenidoover.asp?contenido=93201>

2.5. Grooming.

El *Grooming* es la acción deliberada de un adulto, varón o mujer, de acosar sexualmente a una niña, niño o adolescente a través de un medio digital que permita la interacción entre dos o más personas, como por ejemplo redes sociales, correo electrónico, mensajes de texto, sitios de chat o juegos en línea.⁵⁶

Podemos afirmar que las personas que son actores en esta acción típica son solo adultos que buscan a menores formando un método donde a través de un conjunto de estrategias que una persona adulta desarrolla para ganarse la confianza de un menor de edad a través de Internet y las nuevas tecnologías (TIC), para conseguir su control a nivel emocional, con el fin último de obtener concesiones de índole sexual.

Entre estas estrategias, suelen generar uno o varios perfiles falsos, haciéndose pasar por un niño, niña o adolescente, buscando generar una relación de amistad y confianza con él o la menor a quien quieren acosar. Estos individuos es la siguiente, estos se mantienen merodeando por las salas de chat, redes sociales, foros, o cualquier punto de reunión virtual, con el objetivo de encontrar menores de edad, y ponerse en contacto con ellos. Una vez que logran encontrar a uno, empezarán a hablar con él para ganarse su confianza y hacer que no tenga miedo de ellos, para finalmente revestir con mentiras su deseo real de que satisfagan sus fantasías sexuales, la forma de actuar de estos individuos es muy dispar, desde el simple engaño, a las amenazas contra su vida, la de sus familias, o la más común, la de que, una vez obtenida una fotografía comprometida del menor, la publicarán por todos los medios posibles.

El grooming es un proceso que comúnmente puede durar semanas o incluso meses, variando el tiempo según la víctima. El grooming puede ser considerado un delito de exhibicionismo, difusión de contenidos pornográficos (si se difunden por un medio directo

⁵⁶ Argentina.gob.ar. *Grooming Que es y cómo prevenirlo* [en línea] [consultado el 08 de septiembre de 2023]. Disponible en: <https://www.argentina.gob.ar/grooming#:~:text=El%20GROOMING%20es%20la%20acción,chat%20o%20juegos%20en%20línea.>

y suponen daños psicológicos) y corrupción de menores (si se dan actuaciones de ámbito sexual).

CAPITULO III. ASPECTOS PROCESALES DE LOS CIBERDELITOS RELACIONADOS A LA INTEGRIDAD, INDEMNIDAD Y LIBERTAD SEXUAL.

A lo largo de este trabajo investigativo se ha dejado claro la serie de situaciones, que acarrea una sociedad globalmente interconectada, vinculando a las prácticas y tendencias de las sociedades, que vinculan todo tipo de generaciones o culturas, que producen un cambio de relevancia y alto impacto en la población, a nivel mundial, sobre todo bajo el escenario de un entorno digital, en el que miles de personas se teletransportan a un mundo instantáneo, inmaterial, interactivo y sin ningún tipo de restricción, de bajo costo y menor riesgo.

Anteriormente no se valoraba desde esta perspectiva; pues el código penal “Ley 641” vigente desde el año 2008, dedica el capítulo II a los delitos referidos a la libertad e integridad sexual, y consideramos importante señalar que el Código Penal, tipifica estos delitos como delitos de mera conducta, es decir que requieren de acciones físicas.

Sin embargo, el Código Penal vigente hace referencia a algunos delitos perpetrados a través de las TIC en ciertos artículos y en dos acápites distintos. El primero en el capítulo II Delitos contra la libertad e integridad sexual, ... “*art. 175 Explotación sexual, pornográfica y acto sexual con adolescentes mediante pago*”... tipifica las siguientes acciones: quien promueva, financie, fabrique, reproduzca, publique, comercialice, importe, exporte, difunda, distribuya, material para fines de explotación sexual, por cualquier medio, sea directo, mecánico, digital, audio visual, o con soporte informático, electrónico o de otro tipo⁵⁷ y el ... “*art. 176 Agravantes específicas en caso de explotación sexual pornografía y acto sexual con adolescentes mediante pago*” ...

El Código penal en este sentido, califica hechos delictivos desde una perspectiva no muy propia a las características esenciales de los ciberdelitos. El acervo del legislador por regular estas conductas es el adecuado y se aproxima a la regulación que merecen los

⁵⁷ Resalta que la tipificación establecida en el segundo párrafo del art. 175 CP, en los delitos mediante las TICS, o de forma informática relacionados a la indemnidad sexual, pues el medio y el fin ya sea con objeto comercial o de otra índole, que deben ser acciones punibles, sin embargo, carecen de las directrices debidas que realmente integren a esta legislación elementos y características propias de la nueva forma de actuar criminal.

delitos cometidos por medio de las TICS, sin embargo, intentarlo sin los mecanismos adecuados, es decir sin en abordaje correspondiente o una regulación especial, que requieren esta forma específica de delinquir resulta complicado y ambiguo en la práctica penal.

Continúa el art. 540 del Código Penal, Exhibicionismo “... *Quien se muestre desnudo o exhiba sus órganos genitales en lugares públicos, será sancionado de diez a treinta días multa, o trabajo en beneficio de la comunidad de diez a treinta jornadas de dos horas diarias...*” pese a que no establece propiamente que el medio o la modalidad de comisión de este delito sea mediante el uso de las TICS, anterior a la Ley 1042 se regulaban algunas acciones de esta índole cometidas por medio de las TICS.

El Título III Delitos contra la intimidad y la inviolabilidad del domicilio, del Código penal en los... “*art. 193 sustracción, desvió o destrucción de comunicaciones*”, y “*art. 195 propalación*”... castiga las conductas de hacer público, divulgación, publicación o reproducción y posiciona estos delitos como delitos contra la intimidad y la inviolabilidad de domicilio, de esta manera considero que la fundamentación del injusto penal y el bien jurídico a regular es más la violación a la propiedad como elemento tipificado que la vulneración a la intimidad como tal.

Es por ello, que la forma en que el código penal tipifica, estas acciones informáticas, no salvaguarda, ni atiende en amplio sentido, todo lo que implica el actuar de la tutela penal en los ciberdelitos relacionados a la indemnidad, libertad e integridad sexual, pues resulta exiguo, frente a que no distingue las distintas modalidades, además no predispone los mecanismos necesarios para dar persecución a estos delitos, teniendo en cuenta lo anteriormente expuesto, continuaremos analizando la regulación especial, respecto a los delitos por medio de las TICS.

La ley 1042 fue aprobada el 27 de octubre del año 2020 y publicada en La Gaceta, Diario Oficial N° 201 el 30 de octubre del año 2020, mediante la creación de esta Ley el Estado de Nicaragua, regula de forma especial y asume la protección integral, sancionando a los que utilicen las tecnologías de la información y la comunicación, con fines ilícitos o criminales.

Dentro del objeto de la Ley 1042 “Ley especial de ciberdelitos” art. 3 está la prevención, investigación, persecución, y sanción de los delitos cometidos por medio de las Tecnologías de la Información y la Comunicación, 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, en los términos previstos en esta Ley.

Los delitos de orden informáticos según Oliver Ferreras⁵⁸ ...“tienen como denominador común la utilización de sistemas informáticos, ya sea utilizándolos como medios para cometer delitos o como fines en sí mismos; es decir, siendo los objetivos a los que se dirige la transgresión” ... destacan ser en uno mismo el método, el medio y el fin.

Bajo esta perspectiva el estado actúa como garante de Derechos al reconocer y proteger como tal expresa tácitamente los ciberdelitos en específico los de libertad, e integridad sexual, estableciendo preceptos a las figuras jurídico-penal según el hecho punible.

3.1. Jurisdicción.

La jurisdicción penal se entiende, según lo dispuesto por el art. 18 del CPP *que ...“se ejerce con exclusividad por los tribunales previstos en la Ley, a quienes le corresponde la potestad pública de conocer y decidir en los procesos que se instruyan por los delitos y faltas ...”*

Si bien el concepto de jurisdicción ha venido evolucionando a lo largo de los siglos, en la actualidad se nos presenta como una potestad exclusiva del Estado. La jurisdicción penal, como jurisdicción que es, es una potestad, es decir, es una manifestación de autoridad: el órgano jurisdiccional está en relación de superioridad o supremacía frente a las partes del proceso y a todos los que en él intervengan porque la jurisdicción deriva de la soberanía del Estado. Esta supremacía del órgano jurisdiccional se establece en

⁵⁸ FERRERAS FUENTE, Oliver. “Ciberdelitos. El delio de Intrusismo informático en el ordenamiento jurídico español.” [En línea]. Universidad de León [Fecha de Consulta: 10 de septiembre del 2023]. Disponible en: <https://buleria.unileon.es/bitstream/handle/10612/11363/Fuente%20Ferreras,%20%D3liver%20de%20la.pdf;jsessionid=571334418EEAD46F484CFEB1C01CADF2?sequence=1> P. 12.

pro de la tutela de los derechos de los ciudadanos, de manera que no contradice los postulados de una sociedad democrática⁵⁹.

Esta potestad es pública, puesto que su titular es el Estado, o, más específicamente, determinados órganos del Estado: los tribunales de justicia. Como consecuencia de su naturaleza pública, la potestad jurisdiccional es de ejercicio obligatorio, es un poder-deber. El órgano jurisdiccional no puede negarse a ejercer la jurisdicción cuando se den todos los presupuestos de ella⁶⁰.

3.2. Competencia.

Podemos entender la competencia como la medida en que la jurisdicción se distribuye entre los funcionarios a los que les corresponde la administración de justicia. Es decir que se vincula la jurisdicción y la competencia y no podría existir una sin la otra, sobre todo al tratarse los asuntos procesales.

La ley No 406 “Código Procesal Penal” en el capítulo II distingue tres tipos de competencia: Competencia objetiva⁶¹, competencia funcional⁶² y competencia territorial⁶³ para efectos de competencia objetiva la propia Ley de los ciberdelitos ya la establece en el art. 40⁶⁴.

La competencia objetiva de los juzgados especializados en violencia expresa que Conocen de los hechos cometidos conforme lo establecido en la Ley 1042:

⁵⁹ TIJERINO PACHECO, José María; COLOMER GOMEZ, Juan Luis; PELLENCER BARRIENTOS CRISOSTOMO, R. Cesar et.al. “*Manual de derecho procesal penal*”. 2ª ed. Valencia: TIRANT LO BLANCH, 2006. I.S.B.N.: 84 - 8456 - 549 -1. Pp 92 - 93.

⁶⁰ Idem.

⁶¹ Ley N° 406. “Código Procesal Penal De La República De Nicaragua” SENICSA. Julio 2017. P. 14.

⁶² Ibidem. P. 15.

⁶³ Ibidem. P. 15-16.

⁶⁴ Ley No. 1042, “Ley especial de ciberdelitos.” En la Gaceta Diario Oficial No. 201, del 30 de octubre de 2020, págs. 9318-9326. ... **“Artículo 40 Competencia objetiva En los delitos relacionados en el capítulo V “Delitos informáticos relacionados con la Libertad e integridad sexual” de la presente Ley, cuando sean cometidas contra mujeres, niñas, niños o adolescentes o personas con discapacidad necesitadas de especial protección, serán competentes para conocer y resolver en primera instancia los Juzgados de Distritos especializados en violencia.”** ...

- Artículo 31: Utilización de niñas, niños, adolescentes o personas con discapacidad necesitada de especial protección, en pornografía a través del uso de las Tecnologías de la Información y la Comunicación.
- Artículo 32: Corrupción a personas menores de 16 años o personas con discapacidad necesitada de especial protección a través del uso de las Tecnologías de la Información y la Comunicación.

La competencia objetiva tanto de los juzgados de justicia ordinaria⁶⁵ como los juzgados especializados en violencia

- Artículo 33: Acoso a través del uso de las Tecnologías de la Información y la Comunicación. Quien atormente, hostigue, humille, insulte, denigre u otro tipo de conducta que afecte la estabilidad psicológica o emocional, ponga en riesgo la vida o la integridad física, por medio del uso de las Tecnologías de la Información y la Comunicación, se le impondrá pena de dos a cuatro años de prisión. Cuando la víctima sea niña, niño, adolescente o persona con discapacidad necesitada de especial protección, se impondrá pena de cuatro a seis años de prisión.
- Artículo 34: Acoso sexual a través del uso de las Tecnologías de la Información y la Comunicación. 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 a través del uso de las Tecnologías de la Información y la Comunicación se le impondrá pena de dos a cuatro años de prisión. Cuando la víctima sea menor de 16 años, con o sin su consentimiento o persona con discapacidad necesitada de especial protección se le impondrá pena de cuatro a seis años de prisión.

⁶⁵ Cuando se habla de justicia ordinaria se refiere, a la clasificación de la pena por su gravedad, es decir se valora según la pena si es competencia de los Juzgados Locales o los Juzgados especializados en violencia. Todo conforme la supletoriedad establecida en el art. 45 de la Ley 1042. Y según lo dispuesto en el art. 20, 21CPP es decir cuando se trate de delitos menos graves corresponde la competencia a los Juzgados Locales Penales, y en caso de delitos de penas graves corresponde a razón de competencia a los Juzgados Especializados en Violencia.

- Artículo 35: Condiciones agravantes comunes. Los delitos referidos a los Artículos 31, 32, 33 y 34 serán sancionados con la pena máxima correspondiente, aumentada hasta en una tercera parte del máximo establecido de la pena y la inhabilitación del ejercicio de su profesión durante el tiempo que dure la condena, si cualquiera de las acciones descritas fuera realizado por:
 1. Ascendientes, descendientes, hermanos, cónyuges, conviviente y familiares hasta el cuarto grado de consanguinidad y segundo de afinidad.
 2. Autoridad, funcionarios y empleados públicos.
 3. La persona encargada de la tutela, protección o vigilancia de la víctima.
 4. Toda persona que, prevaleciendo de la superioridad originada por relaciones de confianza, educativa, de trabajo o cualquier otra relación.

3.3. Mediación.

Según el artículo 4 de la Ley de mediación y arbitraje vigente define la mediación: ... “es todo procedimiento designado como tal, o algún otro término equivalente, en el cual las partes soliciten a un tercero o terceros, que les preste asistencia en su intento por llegar a un arreglo amistoso de una controversia que se derive de una relación contractual u otro tipo de relación jurídica o esté vinculada a ellas. El mediador no estará facultado para imponer a las partes una solución de la controversia.” ...⁶⁶

Podemos definir la mediación como aquella manifestación del principio de oportunidad en el ejercicio de la acción penal que consiste en un procedimiento por el cual el imputado y la víctima procuran una solución al conflicto generado por el delito que evite el inicio del proceso penal o su continuación y satisfaga el interés restitutorio o reparatorio de la víctima.⁶⁷

⁶⁶ Ley No. 540, “Ley de mediación y arbitraje.” En la Gaceta Diario Oficial No.122. del 24 de junio del 2005. Pags.4593-4607.

⁶⁷ TIJERINO PACHECO, José María. Ob. Cit. P. 138.

El principio de oportunidad establecido en el art. 14 del Código Procesal Penal se manifiesta con la posibilidad alterna de llegar a acuerdos entre las partes, y para efecto de validez, los acuerdos adoptados por las partes deben de presentarse ante el juez para su debido control de legalidad y en consecuencia su aprobación.

El art. 55 CPP expresamente establece las siguientes formas de manifestaciones del principio de oportunidad:

1. La mediación;
2. La prescindencia de la acción penal;
3. El acuerdo y,
4. La suspensión condicional de la persecución.

El capítulo VIII, de la Ley 1042, en las disposiciones finales, establece en el art. 45 la supletoriedad, es decir que esta Ley puede ser suplida por las demás Leyes correspondientes.

Atendiendo esta disposición y evocando lo establecido en el art. 56 CPP que íntegra y literalmente dice:

“... La mediación procederá en:

1. Las faltas;
2. Los delitos imprudentes o culposos.
3. Los delitos patrimoniales cometidos entre particulares sin mediar violencia o intimidación, y,
4. Los delitos sancionados con penas menos graves.” ...

Conforme estas disposiciones son mediables los delitos sancionados con penas menos graves establecidos en la Ley 1042 primer párrafo siendo los siguientes:

- Art. 32 Corrupción a personas menores de 16 años o personas con discapacidad necesitada de especial protección a través del uso de las tecnologías de la información y la comunicación.
- Artículo 33: Acoso a través del uso de las Tecnologías de la Información y la Comunicación.
- Artículo 34: Acoso sexual a través del uso de las Tecnologías de la Información y la Comunicación.

Acorde la supletoriedad establecida en la Ley 1042, capítulo VIII art. 45, cabe el procedimiento de mediación según lo que dispone el CPP.

Al tratarse de delitos de acción pública contra la integridad y libertad sexual, tal y como lo establece la Ley 1042 en su capítulo V es posible la mediación bien sea previa al proceso, es decir antes de la presentación de la acusación, para evitar el inicio del proceso o durante el proceso, para suspenderlo o poner fin al mismo antes de que se dicte sentencia.

En caso de concurrir con mediación previa, se procederá según lo establecido en el art. 57 CPP es decir que ocurre, antes de la presentación de la acusación o querella; la víctima o el imputado procuran un acuerdo ya sea, ante un abogado o notario debidamente autorizado para mediar, ante la Defensoría Pública o en zonas rurales, ante un facilitador de justicia, acreditado por la Corte Suprema de Justicia.

El acuerdo reparatorio puede ser total o parcial; total cuando se incluyen todos los hechos y personas denunciadas; y parcial, siempre que se trate de varios hechos o personas denunciadas, llegándose a un acuerdo solo por uno o varios delitos, o una o varias personas.

Si el acuerdo preparatorio fuera total, se confeccionará un acta que la partes someterán al Ministerio Público, el cual dentro de un plazo de cinco días deberá pronunciarse sobre su procedencia o no, si no se pronuncia dentro del mencionado plazo, se da por aprobado dicho acuerdo.

Una vez aprobado el acuerdo, el fiscal o cualquier interesado (si aquel no se pronunció), lo presentará al juez competente, solicitando su inscripción en el Libro de Mediaciones previas que lleva el Juzgado competente, así como la suspensión de la persecución penal en contra del imputado por el plazo necesario para el cumplimiento del acuerdo preparatorio.

Si el imputado cumple con los compromisos asumidos en el acuerdo, a solicitud de parte, el juez dictará un auto, que declara extinguida la acción penal. Por el contrario, si el imputado incumplió, a instancia de parte, corresponde al Ministerio Público, reanudar la persecución penal.

Si el acuerdo es parcial, igual al anterior, se levanta acta, se lleva al Ministerio Público, aprobado el acuerdo reparatorio o superado los cinco días que tiene el fiscal para pronunciarse, se presenta ante el juez con la petición que el mismo sea anotado en el Libro de Mediación. Paralelamente, se presentará acusación o querella respecto del hecho donde no se pactó acuerdo.

Mediación durante el proceso.

Esta mediación, es la que ocurre luego de haberse presentado la acusación o querella, es decir, una vez iniciado el proceso penal, sus acuerdos pueden tomarse en cualquier etapa del proceso hasta antes de la sentencia.

Cabe señalar, que, en la mediación durante el proceso, el mediador es el Ministerio Público, a quien debe dirigirse la víctima o el acusado solicitándole el trámite de mediación.

El acuerdo en estos casos también puede ser parcial o total, aprobado por el fiscal se presenta al juez para su anotación en el Libro de Mediación y cumplidos los compromisos, se decretará a instancia de parte, el sobreseimiento respectivo, mientras que el otro u otros hechos (acuerdo parcial) continúan el proceso conforme lo que a Derecho corresponde.

El defensor tiene la obligación de velar por el cumplimiento de todo el trámite de mediación, deberá analizar que:

- Los hechos denunciados configuran un delito.
- La existencia del delito ha sido acreditada.
- Existe suficiente evidencia que incrimina al imputado o acusado.
- El hecho criminal, no es un delito contra el Estado o cometido con ocasión de su ejercicio por funcionarios nombrados por el Presidente de la República o la Asamblea Nacional, o por quienes hayan sido electos popularmente o sean funcionarios de confianza.
- El acuerdo reparatorio es realizado por un mediador autorizado.
- El acuerdo es válido, las partes llegaron a un convenio libre y voluntariamente.

3.4. Procedimiento

Es oportuno resaltar que a la publicación de esta nueva Ley de Ciberdelitos a la par se publicó la reforma de la Ley No. 406, Código Procesal Penal De La Republica De Nicaragua, Ley No. 1060, “LEY DE REFORMA Y ADICIÓN A LA LEY NO. 406, CODIGO PROCESAL PENAL DE LA REPUBLICA DE NICARAGUA” estableciendo cierta especialidad a tomar en cuenta en materia de ciberdelitos.

En vista que no se ha creado un procedimiento especial que realmente guie de forma más específica lo correspondiente a esos delitos tan especiales; la Ley 1042; el capítulo VIII de dicha Ley en las disposiciones finales, establece en el art. 45 la supletoriedad, es decir que lo relacionado al procedimiento de esta Ley puede ser suplida por las correspondientes, atendiendo esta disposición corresponde en su procedimiento lo siguiente.

3.5. Procedimiento Ordinario Por Delitos Graves.

Según lo dispuesto en el Artículo 216 de la Ley 1060⁶⁸ dentro de las cuarenta y ocho horas a la detención o vencido el plazo de la investigación complementaria, el detenido será puesto a la orden del Juez a la celebración de audiencia preliminar. Dicha reforma incluye cierta particularidad al proceso, que podría adquirir ciertas especialidades; una de ella es en el sentido que el Ministerio Público, puede solicitar la ampliación del plazo para investigar y por esa petición efectuada por el Ministerio Público dicha audiencia, podría decirse se transforma y se celebrará inmediatamente “Audiencia Especial De Tutela de Garantías Constitucionales” y la finalidad de la ampliación del plazo es a consideración de que los resultados de la investigación requieren mayor tiempo para complementar la información o los elementos de prueba⁶⁹, con el fin de sustentar la acusación y a la vez la autoridad dicta detención judicial como medida cautelar. Sin embargo, consideramos aquí el legislador incluyo bien podríamos decir otra especialidad pues establece en el mismo artículo ya relacionado que dicha medida cautelar de detención judicial, durará el mismo plazo que se ha fijado para la investigación complementaria.

En cuanto a esta solicitud expresa por el Ministerio Público, el mismo artículo establece debe hacerse de manera oral, o escrita, debidamente fundada y motivada.

Consideramos que estas motivaciones y fundamentación específicamente versan en la prueba, y aquí es necesario recordar lo ya referido por este estudio, debido a la modalidad en este fenómeno jurídico que los hechos en su mayoría de los casos, se consuman en el ciberespacio y por ende la recopilación de la prueba puede iniciarse desde ahí, sin el perjuicio de la incautación de dispositivos informáticos y que la sustracción de la información en el mismo contenga datos efecto de su uso, posible evidencia o el rastreo de la misma. Por lo que se deberá motivar si los datos encontrados

⁶⁸ Ley No. 1060, “Ley de Reforma y Adición a la Ley No. 406, Código Procesal Penal de la República de Nicaragua.” En la Gaceta Diario Oficial, 05 de febrero 2021, No. 25, págs.1023-1024.

⁶⁹ Es decir, para la recopilación de la prueba que sirvan de sustento y fundamenten a la acusación correspondiente por el Ministerio Público, conforme los mecanismos necesarios para su conservación y presentación sobre mecanismos de conservación de la prueba) para el posterior juicio oral y público. Siempre y cuando a consideración de la autoridad judicial reúna los requisitos establecidos por la Ley.

ya sea a través de la red o el propio sistema informático incautado sea el caso, es pertinente para solicitar la ampliación del plazo, y la misma Ley (Art. 256) expresa “cuando se trate de crimen organizado, se trate de delitos de relevancia nacional y trascendencia nacional y cualquier otra información o elemento de prueba que ayude a fundamentar la procedencia de la solicitud.” ...

Cabe recalcar que en la “Audiencia Especial de Tutela de Garantías Constitucionales” deberán estar presentes el Imputado, su defensor y el Ministerio Público. Dado el caso que la autoridad judicial por escucha la fundamentación del Ministerio Público sobre la ampliación del plazo para investigación acceda a la solicitud efectuada por el MP mediante auto debidamente motivado y fundado, en sentido a la gravedad del hecho, complejidad de la investigación, pluralidad de los afectados, imputados y conductas, y sus demás consideraciones pertinentes al caso en específico, y debiendo además en el mismo auto señalar de forma expresa el plazo razonable para la investigación complementaria, y este no podrá ser superior a los 90 días ni menor a 15 días (art. 256 cuarto párrafo).

Continuando con el análisis de este artículo, sexto párrafo consideramos relevante preguntarnos ¿Deberá el ministerio público reportar los avances de la investigación sobre el caso que les atañe a la autoridad judicial? ¿lo puede solicitar la defensa? ¿La autoridad judicial está en el deber de darle seguimiento? ¿en caso de que a consideración de la autoridad judicial es innecesaria la investigación complementaria podrá de oficio ordenar el cese de la misma? El legislador expresa tácitamente: ...“Según el avance de la investigación complementaria si la autoridad judicial consideran innecesario continuar con la detención judicial, será el Ministerio Público, quien solicitaré a la Autoridad Judicial el cese de la misma.”...

En caso de negarse la solicitud efectuada por el Ministerio Publico, se pasa directamente a la correspondiente audiencia preliminar.

Fuera de esas consideradas especialidades incluidas en la reforma, se procede a explicar el procedimiento sin la solicitud de ampliación del plazo de investigación a cargo del MP, por lo que dentro de las cuarenta y ocho horas a la detención o vencido el plazo

de la investigación complementaria, el detenido será puesto a la orden del Juez a la celebración de audiencia preliminar, dicha audiencia que deberá cumplir con las finalidades del art. 255 CPP, siendo las siguientes:

- Hacer de conocimiento del detenido sobre la acusación en su contra, resolver lo referido a medidas cautelares y garantizar el derecho a la defensa.
- El fiscal en esta audiencia está en la obligación de presentar la acusación ante el juez competente debiendo entregar en el acto una copia de la acusación al acusado en caso de no hacerlo se ordena la libertad del acusado. (256 CPP)
- La autoridad judicial examinará si dicha acusación reúne los requisitos del artículo 77 CPP y en caso de reunir todos y cada uno de los requisitos dicta auto de admisión. O en si la rechaza ordena el archivo definitivo.
- En el acto de la audiencia preliminar al momento de que el fiscal de manera sucinta deponga el libelo acusatorio podrá de conformidad al art. 258 correcciones de errores materiales que no impliquen o se consideren ampliación de la acusación. Sin embargo, sin el perjuicio de lo establecido en el art. 259 CPP en cuanto a que en trascurso del proceso antes de juicio, podrá ampliar la acusación mediante la inclusión de un nuevo hecho, y que dicho hecho modifique la calificación jurídica o la pena resulte conexa. Una vez concluida dicha audiencia se señala en el acto fecha para audiencia inicial.

Dentro de las finalidades de la audiencia inicial conforme lo establecido en el art. 265 CCP están las siguientes:

- Determinar si existe causa para proceder a juicio.
- Iniciar intercambio de información sobre pruebas.
- Revisión de medidas cautelares
- Actos procesales que tomaran lugar de previo juicio.

En caso de que la autoridad judicial considere que existen causales suficientes para continuar a juicio Oral y Público, dentro de la misma audiencia inicial se señala fecha del correspondiente debiendo cumplir con las finalidades de lo establecido en el capítulo V del Código Procesal Penal.

3.6. Medidas de aseguramiento y técnicas de investigación.

El Capítulo VI de la Ley 1042, expresa tácitamente en el ... *“art.38 Medidas de aseguramiento: Sin perjuicio de cualesquiera otras medidas de aseguramiento que pudieran contribuir a la persecución efectiva de los delitos comprendidos dentro del ámbito de aplicación de esta Ley, se podrán solicitar las siguientes medidas específicas:*

3.6.1.1. La incautación y depósito de sistemas informáticos o dispositivos de almacenamiento de datos.

4. El sellado, precinto y prohibición de uso de sistemas informáticos o dispositivos de almacenamiento de datos.

5. El requerimiento de preservación inmediata de datos que se hallen en poder de terceros.

6. La copia de datos.

Las medidas de aseguramiento establecidas por la Ley 1042, de la simple lectura se desprenden desde una óptica general, es decir son tratadas de la forma tradicional como la establecida para los delitos comunes, pese a ser delitos en modo y forma especiales, se puede interpretar que estas medidas específicas, son de ejecución personal, efectuada por el órgano responsable de las actividades de investigación para el descubrimiento y comprobación de hechos, según lo dispuesto en el art. 228 CPP por la Policía Nacional, es decir, se requiere que oficiales o el equipo técnico de investigación se traslade hasta la escena del crimen (en caso de existir) donde se perpetua el delito consumado y en efecto proceder con la incautación, deposito, sellado, precinto, prohibición, preservación, requerimiento y copia de datos.

Sin embargo, con estos delitos, resulta en ciertos aspectos inaplicable los métodos usuales empleados para delitos comunes, con técnicas de investigación tradicionales, en la etapa de investigación o recopilación de la prueba confiada a la Policía Nacional, al momento de dar persecución a estos tipos penales. Pero no significa que no sean valiosas, o que se deban invalidar estas técnicas de investigación, lo que se debe

considerar si es lo pertinente al delito aplicable; es el tratamiento de estos delitos, teniendo presente que usualmente se cometen en el ciber espacio, por ende, se debe contar con especialistas que puedan efectuar la persecución penal en el mismo.

La creación de esta Ley, estima conveniente a la par, la creación especial de organismos o bien sea de unidades especializadas dentro del cuerpo de la Policía Nacional, sobre todo, la conformación de equipos técnicos encargados de prevenir, proteger y refrenar la ola ciber delictiva. Al Corresponderle a la Policía Nacional iniciar de inmediato la investigación y comprobación de hechos, resulta grave el no contar con las medias técnicas, o tácticas que procuren el aseguramiento de indicios y evidencias relacionadas al hecho presuntamente delictivo que investigan. El no contar con un equipo técnico de investigación especializado en materia informática, con funciones, técnicas especiales investigativas y medidas establecidas, es en efecto una ventaja para el o los autores directos en cualquier ciberdelito, permitiéndoles el tiempo suficiente para movilizarse, desaparecer, ocultar, eliminar o destruir evidencia que pueda existir dentro un dispositivo electrónico.

Es por ello por lo que debe considerarse la creación de un instructivo especial para el ente encargado de la investigación y por ende la conservación de la prueba, sin embargo, dicha Ley omite por completo las técnicas necesarias y especiales de persecución a esta nueva modalidad criminal.

En España por ejemplo, se ha considerado elemental tomar medidas y técnicas de investigación para la persecución penal de estos delitos, acordes a la modalidad criminal que enfrentamos, en este sentido, Josefina Quevedo⁷⁰ en su análisis de tesis doctoral, advierte de la problemática de los instrumentos de investigación tradicionales, y en ese sentido su legislación dio respuestas mediante una reforma a la Ley Orgánica de octubre del año dos mil quince y expresa tácitamente las siguientes medidas de aseguramiento:

⁷⁰ GONZALEZ QUEBEDO, Josefina. *“Investigación y prueba del ciberdelito”*. Tesis Doctoral , Universidad de Barcelona, 2017. Pp.171 – 172.

- a) La interceptación de las comunicaciones telefónicas y telemáticas como vía de investigación criminal de los ilícitos que se cometen a través de la red.
- b) Captación y grabación de comunicaciones orales abiertas mediante el empleo de dispositivos electrónicos.
- c) La identificación de equipos o usuarios a partir de una dirección IP⁷¹.
- d) Identificación de terminales mediante captación de códigos de identificación del aparato y sus componentes.
- e) Identificación de titulares o terminales de dispositivos de conectividad.
- f) Utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen.
- g) El registro de dispositivos informáticos de almacenamiento masivo y el registro remoto de equipos informáticos.
- h) La actuación bajo identidad supuesta en los canales cerrados de comunicación telemática, mediante la regulación del *agente encubierto informático* y para la grabación de imágenes y conversaciones, cuando fuera preciso. En ambos casos, la necesidad de autorización judicial garantiza el pleno respeto del Derecho a la intimidad y al secreto de las comunicaciones de las personas afectadas.

En ese sentido, teniendo en cuenta la realidad jurídica de acuerdo a las posibilidades y retos que enfrenta la legislación nicaragüense, es de considerarse vital, útil y pertinente para la persecución de estos delitos la identificación de una dirección IP dichas direcciones no simplemente son la representación numérica de donde está conectado un dispositivo, a través de ella se puede tener una localización cercana del dispositivo

⁷¹ Avast Software s.r.o. “¿Qué es una dirección IP? [en línea] [fecha de consulta: 11 de septiembre 2023]. Disponible en: <https://www.avast.com/es-es/c-what-is-an-ip-address> ... “Una dirección IP es una representación numérica del punto de Internet donde está conectado un dispositivo. Se usa para identificar dónde hay algo y, en cierto modo, qué es. Comprender los fundamentos de las direcciones IP es esencial para desenvolverse por Internet. Aprenda cómo funcionan las direcciones IP y por qué es tan importante proteger la suya.” ...

de donde se está navegando, el sistema operativo que se está usando, una persona con los conocimientos mínimos si la conexión a internet no está cifrada fácilmente puede acceder y espiar tus actividades, a través de los mismos sitios web que visitas puede ver todo lo que entra y sale de su equipo.

Por ejemplo, al estar tu dirección IP visible en tu ordenador personal, puedes dejar tu correo abierto, es común guardar contraseñas, vincular tu cuenta de navegador, incluso utilizar como herramientas para él envío de documentos, como las redes sociales que almacenan datos como: Telegram, Wathsap Web, Facebook o demás redes sociales, chatear desde el mismo ordenador, el, incluso conectarte a la red de por ejemplo una cafetería dicha red se vincula incluso con los demás dispositivos que se conectaron a la misma red.

Otro que podría considerarse relevante es la identificación de terminales mediante la captación de códigos del aparato o de sus componentes, nos referimos a los datos indicativos de cualquier aparato o dispositivo electrónico, su código de fabricación para identificar el equipo utilizado para acceder a la telecomunicación y una vez con dichos datos se podría vale de la ayuda de los servidores de las telecomunicaciones, para que la policía proceda a intervenir y dar con los dispositivos.

3.7. Conservación de Datos

La Ley 1042 establece en el art. 37 Conservación de datos: La policía Nacional o el Ministerio Publico, en el ámbito de su competencia, actuaran con la celeridad requerida para conservar los datos contenidos en un sistema de información, sus componentes, o los datos de tráfico del sistema, principalmente cuando estos sean vulnerables a su pérdida o modificación.

En este sentido atendiendo la literalidad de la norma, se refiere a la conservación de datos o el tráfico cuando sean vulnerables a su perdida y modificación, para ello por lógica jurídica es necesaria la intervención material o física de la Policía Nacional y Ministerio Publico. A fin de tener claro, a que se refiere nuestra legislación con la

conservación de datos en un sistema de información; empezaremos definiendo que es un sistema de información.

Según el Sistema de integración Centro Americano SICA “Por definición es un conjunto de elementos que interactúan entre sí con un fin común; que permite que la información esté disponible para satisfacer las necesidades en una organización, un sistema de información no siempre requiere contar con recuso computacional, aunque la disposición del mismo facilita el manejo e interpretación de la información por los usuarios.

... “Los elementos que interactúan entre sí son: el equipo computacional (cuando esté disponible), el recurso humano, los datos o información fuente, programas ejecutados por las computadoras, las telecomunicaciones y los procedimientos de políticas y reglas de operación.

Un Sistema de Información realiza cuatro actividades básicas:

- Entrada de información: proceso en el cual el sistema toma los datos que requiere.
- Almacenamiento de información: puede hacerse por computadora o archivos físicos para conservar la información.
- Procesamiento de la información: permite la transformación de los datos fuente en información que puede ser utilizada para la toma de decisiones
- Salida de información: es la capacidad del sistema para producir la información procesada o sacar los datos de entrada al exterior.

Los usuarios de los sistemas de información tienen diferente grado de participación dentro de un sistema y son el elemento principal que lo integra, así se puede definir usuarios primarios quienes alimentan el sistema, usuarios indirectos que se benefician de los resultados pero que no interactúan con el sistema, usuarios gerenciales y

directivos quienes tienen responsabilidad administrativa y de toma de decisiones con base a la información que produce el sistema.” ...⁷²

Resulta un tanto somero el manifiesto como tal, en lo establecido por dicho artículo sobre la conservación de datos en la Ley 1047, siendo que se requieren más aspectos que los generales ya establecidos, aquí la importancia al momento de garantizar en la etapa investigativa los elementos y herramientas pertinentes que ayuden no solamente a su conservación; si no, su protección, sobre todo para la cadena de custodia y su posterior incorporación a juicio, salvaguardando así los elementos de convicción que serán probados.

La doctrina distingue tres tipos en la conservación de datos:

3.8. Conservación de datos de contenido.

Ese tipo de datos podría asociarse a la interceptación de datos en tiempo real, a la comunicación o a un sistema informático en el desarrollo de la investigación, con el fin de obtener, gravar y recopilar la prueba ...“Los datos de contenido constituyen la información que se comunica y se trasmite...”⁷³.

Por lo que se encuentra A disposición de Contenido lo siguiente:

- mensajes/correos electrónicos disponibles en la cuenta de correo del usuario. •
- Archivos adjuntos, fotos, videos y grabaciones de audio.
- Lista de contactos
- Borrador de correo electrónico
- Grabaciones

⁷² Guatemala. Instituto De nutrición De Centro América Y Panamá [en línea] [fecha de Consulta: 19 de septiembre del 2023]. Disponible en: <http://www.incap.int/sisvan/index.php/es/acerca-de-san/797-sin-categoria/501-sistema-de-informacion>.

⁷³ QUEVEDO GONZÁLEZ, Josefina. Loc. Cit. P.185.

- Videos
- Enlaces de un servidor web.
- Correo electrónico eliminado disponible
- Copia de seguridad/registro de mensajes
- Otros registros relacionados con la cuenta o el servidor solicitado⁷⁴

3.9. Conservación de datos de tráfico.

El convenio de Budapest define los datos de tráfico, en el artículo 1 “...por «*datos sobre el tráfico*» se entenderá cualquier dato informático relativos a una comunicación por medio de un sistema informático, generados por un sistema informático como elemento de la cadena de comunicación, que indiquen el origen, destino, ruta, hora, fecha, tamaño y duración de la comunicación o el tipo de servicio subyacente...” es decir vienen a ser los rastros de navegación que aportan información fundamental por ende prueba sobre el origen de la comunicación, los destinos entre dispositivos a través de la red.

Los datos de tráfico, o metadatos, en una comunicación son los datos que rodean el mensaje que se transmite, pero que no forman parte de dicho mensaje. Son un subproducto de las conexiones, que se concretará en función del tipo de comunicación. Así, en una llamada telefónica, se trata del número de teléfono de llamada, el nombre y la dirección del abonado de origen, el número de destino y el nombre y dirección del abonado de destino, la fecha y hora del comienzo y fin de la comunicación, el servicio telefónico utilizado, y otros datos específicos de la telefonía móvil (la identidad internacional del abonado [IMSI] que llama y del que recibe la llamada; la identidad internacional del equipo móvil [IMEI], también del que llama y del que recibe la llamada; si el servicio es de pago por adelantado: fecha y hora de la primera activación del servicio

⁷⁴ *La Conservación De Datos Informáticos El Uso De Las Redes Internacionales 24/7 Y G/7 La Solicitud De Asistencia Judicial Internacional En El Marco De La Ciberdelincuencia*. Ministerio Público de Fiscalía de la Nación. Julio, No. 1. Lima, Perú: Unidad de cooperación judicial internacional y extradiciones, 2021. Disponible en <https://www.gob.pe/institucion/mpfn/informes-publicaciones/2116853-boletin-informativo-n-1-conservacion-de-datos-redes-internacionales-y-cooperacion-internacional> P. 2

y la etiqueta de localización o identificador de celda desde la que se haya activado el servicio). En cambio, en el acceso a internet y en el correo electrónico serán metadatos, tanto para el origen como para el destino de la comunicación, la identificación de usuario asignada, el nombre y la dirección del abonado o usuario al que se le ha atribuido una dirección de protocolo internet (IP); la fecha y hora de conexión y desconexión del servicio de acceso a internet; el servicio de internet utilizado; o la línea digital de abonado (DSL). Téngase en cuenta que la dirección del protocolo internet puede ser dinámica o estática, en función de la asignación que realiza el proveedor de acceso. Estamos incluyendo parte de los datos de localización en los datos de tráfico, porque son tratados en la conducción de una comunicación.

Como se ve, estos datos accesorios a la comunicación detallan quién, cuándo, dónde y con quién se produce esta sin entrar en su contenido. En general estamos ante unos datos de abonados y usuarios que son necesariamente tratados por los proveedores de comunicaciones para efectuar la propia comunicación, pero que son susceptibles de ser usados de formas muy diferentes, a la vez que pueden agredir los derechos fundamentales.

Téngase en cuenta que los metadatos⁷⁵ aluden a una comunicación concreta, siendo diferentes a otros datos o circunstancias personales que tendrán los operadores, pero que son autónomos y se hallan desconectados de una comunicación (esta distinción también se refleja en alguna jurisprudencia, como en la Sentencia del Tribunal Supremo español 247/2010, de 18 de marzo, FJ 3). De todos modos, alguno de estos datos de suscripción o abonado podrían ser también datos de tráfico al ser tratados como tales en el curso de una comunicación.⁷⁶

⁷⁵ RAVENTOS PAJARES, Pepita. Los metadatos: que son y para que sirven. *Revista d'arxiux* [en línea]. 2009, Núm. 8, P. 11 [fecha de consulta: 15 de septiembre del 2023]. ISSN: 1696-1552. Disponible en: <http://arxivervalencians.org/wp-content/uploads/2017/02/revista2009.pdf> ...“Los metadatos son información estructurada que describe, explica, localiza, o hace más fácil de recuperar, utilizar o manejar una fuente de información. A los metadatos, a menudo se les llama datos que se usan para describir otros datos. Es el uso más tradicional del término.”

⁷⁶ FERNÁNDEZ RODRÍGUEZ, Jose Julio. J. Los datos de tráfico de comunicaciones: En búsqueda de un adecuado régimen jurídico que elimine el riesgo de control permanente. *Revista Española de Derecho*

En consecuencia, se pueden conservar los siguientes datos de tráfico:

- IP de conexión de publicaciones y/o mensajes enviados
- Hora y fecha de conexión
- Hora y fecha de desconexión
- Nombre y detalles de identificación de personas que accedieron a una imagen, archivo o página web específica entre un periodo de tiempo y fecha específica.
- Método de conexión (<https://>)⁷⁷

¿Porque son importantes jurídicamente? recopilan información que puede formar bases para una investigación, y elementos de convicción que contribuyan a revelar aspectos, como manías, vida privada, la frecuencia en que ese hace algo, la manera en que se puede identificar, de esa manera se podría tener acceso incluso al GPS que se sabe la geolocalización desde donde se efectúa la comunicación.

3.10. Conservación de datos de abonados.

Finalmente, los denominados «datos de suscripción» o «datos de abonado», clase de datos que constituyen «la información personal recabada del abonado a la hora de suscribir el contrato de prestación de servicios de comunicación». Puesto que tales datos son previos a la comunicación y se hallan desligados de la realización en tiempo real de ésta, a priori en ningún caso, atendido el criterio para delimitar los datos de tráfico a que nos hemos acogido, deberían incluirse dentro del contenido de la misma. Una vez más, sin embargo, nos vemos en la obligación de rechazar tan tajante afirmación, ya que nada impediría que ciertos datos que pueden incluirse en esta categoría (como los relativos al «tipo de comunicación usado» o «datos de localización del equipo terminal») sean tratados como datos de tráfico, es decir, accesoriamente al contenido material, en el curso de una comunicación.

Constitucional [en línea]. 2016, No. 108, 93-122. [fecha de consulta: 16 de septiembre del 2023]. ISSN-L: 0211-5743 Disponible en: <http://dx.doi.org/10.18042/cepc/redc.108.03>

⁷⁷ Guatemala. Instituto De nutrición De Centro América Y Panamá. Loc. Cit. P. 2.

La trascendencia de estos datos desde la perspectiva procesal penal radica en las características de la delincuencia que se sirve de las nuevas tecnologías facilidad para la destrucción de pistas, flexibilidad y velocidad en las aplicaciones, carácter transfronterizo, intervención de múltiples agentes públicos y privados, etc., que obligan a las autoridades encargadas de la prevención y persecución penales a dotarse de nuevos medios de lucha contra ella.

Es a los fines de hacer posible el «principio de trazabilidad» y, en definitiva, de superar los obstáculos que las nuevas tecnologías conllevan para la identificación de los autores de hechos delictivos o para la obtención de rastros que conduzcan a ellos, que se reclama la conservación de los datos aparejados a las comunicaciones, de cuyo oportuno entrecruzamiento y empleo debe derivarse la obtención de una información adecuada para localizar, identificar o descubrir a los autores de delitos que se sirvan de las comunicaciones electrónicas a efectos de cometerlos⁷⁸.

Se puede conservar la siguiente información.

- Nombre y la dirección del usuario
- Fecha de nacimiento
- Fecha y hora de suscripción y tipo de registro
- Periodo del servicio • Número de teléfono
- Dirección de correo electrónico
- La dirección de protocolo de internet (IP) utilizada por el usuario para registrar la cuenta o iniciar el servicio
- Información sobre la facturación y medio de pago.⁷⁹

3.11. Aspectos Generales de la Prueba.

⁷⁸ GONZÁLEZ LÓPEZ, Juan José. “La retención de datos de tráfico de las comunicaciones en la Unión Europea: una aproximación crítica” (en línea]. Editorial LA LEY. Universidad de Burgos. 15/12/2017. [fecha de consulta: 17 de septiembre del 2023]. Disponible en : https://www.ubu.es/sites/default/files/portal_page/files/la_retencion_de_datos_de_trafico_de_las_comunicacac..pdf. P.2.

⁷⁹ Guatemala. Instituto De nutrición De Centro América Y Panamá. Loc. Cit. P. 2

Atendiendo el Derecho común, a disposición de lo establecido en el art. 15 del CPP “Cualquier hecho de interés para el objeto del proceso puede ser probado por cualquier medio de prueba lícito. La prueba se valorará conforme el criterio racional observando las reglas de la lógica” en este sentido por la modalidad del tipo delictivo, las evidencias digitales adquieren total protagonismo pragmático, pues será en su mayoría esta la forma de su obtención.

Tomando en cuenta la peculiaridad propia de estos delitos, no es fácil la obtención de las evidencias digitales y de igual forma de toda la recopilación de información, generada y almacenada dentro de la presencia de dispositivos de naturaleza digital, sobre todo que en su mayoría se refugian bajo la animosidad. Ante tal carencia de mecanismos y de elementos de convicción, el hecho delictivo no llega al conocimiento judicial, por tanto, es necesario hacer énfasis en la recopilación y obtención de la prueba digital.

Ya en los capítulos anteriores se trató una de las características de los ciberdelitos como es la instantaneidad, por tanto, a medida que se desarrolla la etapa investigativa y la recopilación de pruebas se corre el riesgo de su manipulación, alteración o desaparición. Aquí radica la importancia en ser lo suficientemente ágiles y poder contar con los recursos necesarios para acceder a datos y conservarlos a la disposición judicial.

Siendo sugestivos en la actividad probatoria, específicamente en la etapa investigativa para el posterior ofrecimiento y admisión de la prueba, como ya se mencionó anteriormente gracias a la reforma del Código Procesal Penal mediante la Ley 1060⁸⁰ en la que mediante audiencia especial de Tutela de Garantías Constitucionales el Ministerio Público, podrá solicitar la ampliación del plazo para investigar y se dicte detención judicial, siempre que se considere que los resultados de la investigación requieren mayor tiempo para complementar la investigación o hacerse de más elementos de prueba para sustentar y formular acusación contra una o varias personas.

Recordando lo dispuesto en el art. 7 del CPP uno de los fines del proceso penal es el esclarecimiento de los hechos y la determinación de la responsabilidad de los acusados,

⁸⁰ Ley No. 1060. Ob. Cit.

sin embargo, tomando en cuenta los nuevos límites de estos delitos, el abanico de posibilidades y artimañas que pueden emplearse con la especialidad de estos delitos conviene preguntarnos, ¿qué puede ser probado? ¿Cuál puede ser la fuente de la prueba? ¿Cuál es el medio de prueba?

3.12. Características de los medios de prueba

Las pruebas electrónicas, poseen una serie de características que son importantes de analizar, con el fin de tener un mejor contexto sobre el tema.

- Parciales: En algunas de las circunstancias, los medios electrónicos que contienen evidencias se encuentran en poder de las personas que quieren presentarlas como pruebas.
- Destruibles: Una prueba electrónica se puede destruir con un solo clic y para poderla recuperar se debe contar con la ayuda de un perito calificado.
- Transgresivas: La obtención de material probatorio electrónico puede trasgredir derechos y libertades fundamentales como el de la libertad, intimidad protección de datos etc.
- Intangibles: Por el solo hecho de estar en el ciberespacio, tienen esta característica, recordando que el mismo se encuentre en números binarios.⁸¹

Sin embargo, la UNODC manifiesta las siguientes características de la evidencia digital:

Admisible: Ajustarse a las normas, antes de ser sometida a un tribunal.

- Auténtica: Posibilidad de vincular la materia probatoria al incidente.

⁸¹ LOPEZ, Jesica, FIGUEROA SÁENZ, Mónica. *“La Obtención De La Prueba Penal Internacional En Materia De Delitos Cibernéticos”* [en línea]. Monografía de grado para optar a título de abogado inédita, Universidad politécnico Gran Colombiano, Bogotá, 2018. [fecha de consulta: 20 de septiembre del 2023]. Disponible en: <https://alejandria.poligran.edu.co/bitstream/handle/10823/1501/Ciberdelitos%20%28Monica%20Senz%20-%20Jessica%20Lopez%29-Ultima%20version%20corregida.pdf?sequence=1&isAllowed=y> P 32.

- Completa: debe contar con toda la historia y no solo con una perspectiva particular.
- Confiable: No debe haber duda de cómo fue recogida y posteriormente manipulada.
- Creíble: Debe ser fácilmente creíble y comprensible por un tribunal.⁸²

3.13. Elementos de convicción.

Como se ha venido recalando es una nueva modalidad de efectuar delitos y resulta interesante preguntarse, sobre los mecanismos con los cuales se busca constatar los hechos controvertidos objeto de investigación, cuando en su mayoría se cometen en el ciberespacio⁸³.

No es de menospreciar y mucho menos desechar el soporte tradicional, en los elementos de convicción que sirven para esclarecer los hechos, solo que no debemos considerar dentro de este contexto únicamente, la prueba testimonial, la prueba documental y la prueba pericial, en este sentido nos referimos a que es vital la evidencia digital, entre ellas están:

Sistemas de Computación Abiertos:

Son aquellos que están compuestos de las llamadas computadores personales y todos sus periféricos como teclados, ratones y monitores, las computadoras portátiles, y los servidores. Actualmente estos computadores tienen la capacidad de guardar gran cantidad de información dentro de sus discos duros, lo que los convierte en una gran fuente de evidencia digital.

Sistemas Convergentes de Computación:

⁸² UNODOC. “Aspectos básicos de la investigación que involucra Prueba Digital” Panamá, Julio 2021. P.25 [en línea] [consultado el: 20 de septiembre del 2023]. Disponible en : https://www.unodc.org/documents/ropan/2021/PANZ41/Aspectos_basicos_de_la_investigacion_que_involucra_prueba_digital.pdf

⁸³ Ibidem. P 17.

Son los que están formados por los teléfonos celulares llamados inteligentes o SMARTPHONES, los asistentes personales digitales PDAs, las tarjetas inteligentes y cualquier otro aparato electrónico que posea convergencia digital y que puede contener evidencia digital.

- Smartphone: Teléfono inteligente, BlackBerry
- Smart tv: Televisores inteligentes
- PDAs: Un asistente personal digital (PDA), también conocido como un paquete con una PDA o asistente personal de datos , es un dispositivo móvil que funciona como un administrador de información personal, que a menudo tiene la capacidad de conectarse.
- Tarjeta inteligente (smart card), o tarjeta con circuito integrado (TCI), es cualquier tarjeta del tamaño de un bolsillo con circuitos integrados que permiten la ejecución de cierta lógica programada.

Aparatos electrónicos con convergencia digital: Aparatos que en forma tradicional han sido utilizados para un fin específico se hayan transformado de tal manera que se pueden realizar con ellos funciones distintas a su uso nativo⁸⁴.

3.14. Naturaleza Jurídica de la prueba en los Ciberdelitos

En materia penal, la prueba se centra bajo ciertas directrices o distinta metodología, que hace particular los elementos probatorios, desde su recolección y la cadena de custodia es sabido requiere de órganos encargados de presévalos para que mantengan su validez y eficacia.

Por ello la Msc. Martha Lorena Quezada Saldaña considera: ...“La presente Ley 1042, Ley Especial de Ciberdelitos, tutela derechos fundamentales de los ciudadanos y ciudadanas nicaragüenses como son: la intimidad de las personas, sus datos,

⁸⁴ Idem. Loc. Cit. P. 26-27.

información, inviolabilidad de su correspondencia, comunicación, su patrimonio, libertad e Integridad sexual, todos son derechos humanos de rango constitucional.

Además, tutela bienes jurídicos de la Seguridad Nacional, siendo estos: El Espacio, ahora con el desarrollo de las Tecnologías de la Información y la Comunicación, surge un nuevo bien a proteger el Ciberespacio, donde se desarrollan todas las acciones virtuales, que realizan las personas que utilizan las herramientas de la Internet, incluyendo aquellas acciones virtuales ilícitas objeto de esta ley.

En ese mismo orden se tutela la Telecomunicaciones, su seguridad y buen desarrollo, la protección a los datos e información que manejan las Instituciones Públicas, e incluso la información militar de Estado. Por todos estos motivos expuestos es que se ubica esta ley como de orden Público, su persecución es de oficio. (arto.2 de la Ley 1042 “Ley Especial de Ciberdelitos”)⁸⁵

Reformas recientes.

La Asamblea Nacional en Nicaragua aprobó por unanimidad la Ley No. 1219, Ley de Reformas y Adiciones a la Ley 1042, Ley Especial de Ciberdelitos, publicada en la gaceta No. 170 del doce de septiembre del dos mil veinticuatro.

En esta reforma de Ley se incluyen aquellos delitos que se puedan cometer, a través del uso de redes sociales y aplicaciones móviles, en perjuicio de personas naturales o jurídicas, así como la protección integral de los sistemas que utilicen dichas tecnologías, su contenido y cualquiera de sus componentes.

La nueva Ley castiga con cárcel y multas a quienes, en el país o en el exterior, difundan en redes sociales publicaciones que causen «alarma, temor, pánico o zozobra» entre la población.

En relación a los delitos contra la libertad e integridad sexual, el cual es nuestro objeto de estudio, la reforma consistió únicamente en agregar el tratamiento procesal de la responsabilidad penal de las personas jurídicas de los delitos relacionados con la libertad

⁸⁵ QUEZADA SALDAÑA, Martha Lorena. Ob. Cit. P. 25.

e integridad sexual a través del arto. 34 *bis en* relación con el arto. 45 *bis* del código penal, sin embargo, no agrego nuevos delitos al capítulo V de la Ley.

DISEÑO METODOLÓGICO

Tipo de investigación.

En base al análisis de los ciberdelitos relacionados a la libertad, indemnidad e integridad sexual, y conforme el estudio de nuevos términos jurídicos, a razón de una Ley especial de ciberdelitos, es de **tipo teórico documental** y **dogmática jurídica** por lo que se desarrolla, mediante el estudio de antecedentes, análisis y recopilación de datos; que permiten redescubrir, interpretar y construir bajo un nuevo contexto diferentes aspectos de la investigación y su perspectiva jurídica.

Área de investigación.

De conformidad con el reglamento de investigación de la unan León, el área general de la presente investigación es: Estado de derecho, gobernabilidad y democracia; y de conformidad con las líneas de investigación aprobadas por la Facultad de Ciencias Jurídicas y Sociales, el área específica es la de las Ciencias penales, dentro de esta área se abarcan el derecho penal sustantivo y adjetivo.

Enfoque de la investigación.

Este estudio tiene un enfoque cualitativo, porque pretende describir lo relacionado al fenómeno de los ciberdelitos y su regulación en la legislación nacional, desde una perspectiva dinámica de interpretación, con el objeto de comprender mejor el fenómeno de los ciberdelitos.

Método de Investigación: La metodología a emplear, en la presente investigación, consiste en el método deductivo, dado que se pretende partir del estudio de lo general a lo particular, a fin de garantizar su correcta síntesis, mediante conclusiones válidas.

Tipos de métodos:

- Histórico-Lógico.

Este método permite visualizar, y tener un punto de referencia, en el estudio y desarrollo de esta investigación, pues permite conocer el comportamiento histórico del uso del

internet desde su nacimiento, hasta su proceso evolutivo, con la nueva modalidad de cometer delitos. Además de dar a conocer nuevos términos resalta y enfoca aspectos básicos que permitan una mejor comprensión de nuevos delitos.

➤ Método deductivo.

Esta investigación tiene como objeto analizar los ciberdelitos, partiendo de lo general a lo particular, centrándose en los ciberdelitos de carácter sexual, a los cuales podría considerársele delitos sexuales informáticos.

Debido al creciente aumento de las tecnologías de comunicación, se establecen nuevas formas de cometer delitos, pero en particular los ciberdelitos relacionados a la integridad sexual, el delito como tal es tradicional, sin embargo, para la comisión de estos, cambia en modalidad y características, con este método se pretende deducir cuáles son esas nuevas modalidades y características que nacen de las tecnologías de comunicación.

➤ Método de análisis- síntesis.

Para este estudio que parte, del análisis de un nuevo fenómeno jurídico, es fundamental, la recopilación de datos, información o documentos particularmente, de los ciberdelitos, su modalidad, sus características, y la forma en que el Derecho debe tratar estos nuevos riesgos delictivos.

Plano epistemológico.

Debido al enfoque de la investigación, el plano epistemológico es sociológica jurídica, porque permite el análisis desde que se origina el fenómeno jurídico, su evolución, hasta transformarse en una nueva modalidad de comisión de delitos, además permite a través de su estudio, comprender mejor este nuevo fenómeno jurídico.

Nudos cognitivos.

- Teórico-especulativo.

A partir del estudio de nuevos aspectos conceptuales en el Derecho, sobre los ciberdelitos, permite a esta investigación enfocada en la regulación del nuevo fenómeno jurídico, aportar nuevos términos y sustentar su trato procesal.

- Jurídico-histórico

Debido a que este estudio advierte una regulación más compleja, y especializada por tratarse de ciberdelitos en específico los relacionados a la libertad, indemnidad e integridad sexual, es necesario conocer los aspectos evolutivos desde la creación de internet, su incidencia en los delitos sexuales informáticos y la regulación en Nicaragua.

- Jurídico-sociológico

Debido a que el origen de las normas nace de acuerdo con la necesidades y comportamiento de la sociedad, es necesario conocer como el hecho del crecimiento de la sociedad junto a las TIC dan origen a una normativa con el deber de proteger nuevos derechos como lo son los derechos informáticos y comprender el comportamiento de los ciudadanos ante el ordenamiento jurídico.

- Jurídico-dogmático

Se encuentra presente en este estudio, el estudio de la legislación, y el análisis de la Ley sometida a la interpretación y su relación instantánea al momento de la persecución e inicio del proceso que se realiza por la institución correspondiente.

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.

Los Ciberdelitos de relacionados con la indemnidad, libertad e integridad sexual están contenidos en el capítulo V de la ley 1042, “Ley Especial de Ciberdelitos” , regulados del artículo 31 al 35 y se reducen básicamente a tres, a)- la utilización de niñas, niños, adolescentes o personas con discapacidad necesitada de especial protección, en pornografía a través del uso de las Tecnologías de la Información y la Comunicación, b)- la corrupción a personas menores de 16 años o personas con discapacidad necesitada de especial protección a través del uso de las Tecnologías de la Información y la Comunicación, y c)- el Acoso sexual a través del uso de las Tecnologías de la Información y la Comunicación.

Del análisis típico realizado podemos decir que estos tipos de delitos son de naturaleza especial , tanto por el sujeto activo que los realiza, como por el modo o forma de comisión, sin embargo podemos observar mucha debilidad en la técnica de redacción de estos tipos penales en Nicaragua , algunos son incompletos e imprecisos, otros son poco claros, al parecer el legislador los redactó de forma apresurada sin hacer un buen análisis de derecho comparado para luego ajustarlo a la realidad nicaragüense, por lo que consideramos que se debe mejorar su redacción y se debe incluir en la Ley otros delitos que a nivel mundial ya están siendo incorporados en otras legislaciones.

En cuanto a su tratamiento procesal pudimos observar que lamentablemente no tienen un tratamiento procesal especial , ni en la investigación policial, ni en el procesamiento jurisdiccional, y recordemos que por su forma de comisión que es en el ciberespacio se tendría que requerir técnicas mas especializadas en la investigación y por lo menos reglas de procesamiento jurisdiccional más especiales , actualmente estos delitos se juzgan con las reglas del proceso ordinario contenidas en el Código Procesal Penal.

FUENTES DE LA INFORMACIÓN.

FUENTES PRIMARIAS

Tratados

- Convenio sobre la ciberdelincuencia, aprobado por el Comité de ministros del Consejo de Europa en su 109ª reunión, el 8 de noviembre de 2001. El 23 de noviembre de 2001 se abrió a la firma en Budapest y entró en vigor el 1 de julio de 2004.

Leyes

- Constitución Política de Nicaragua, Aprobada el 9 de enero de 1987, publicada en la Gaceta, Diario Oficial No. 5, con reforma el 21 de enero de 2014, publicada en la Gaceta, Diario Oficial No. 26.
- Ley 1042, “Ley especial de Ciberdelitos”, Aprobada el 27 de octubre de 2020, Publicada en La Gaceta, Diario Oficial No. 201 de 30 de octubre de 2020.
- Ley N° 406, Código Procesal Penal De La República De Nicaragua, Publicada En La Gaceta, Diario Oficial N° 243 Del 21 De diciembre De 2001 Y N° 244 Del 24 De diciembre De 2001.

FUENTES SECUNDARIAS.

Doctrina

- ANDRÉS BARRIOS, Moisés. “*Delitos 2.0: aspectos penales, procesales y de seguridad de los ciberdelitos*”. [en línea] 1ª ed. Madrid: Wolters Kluwer España, 2018. [fecha de consulta: 25 de agosto del 2023]. ISBN 978-84-9020-744-4. Disponible en: E Libro.
- ÁLVAREZ, Teodoro Javier. “*Delitos Sexuales Coerción sexual e internet Grooming-Sexting- Sextortion- Stalking*”. 1ª ed. Buenos Aires: Ediciones DyD, 2018. ISSN: 978-987-9371-85-5.
- ALBARRÁN RUFIAN, Mikel. “*La importancia del ciberespacio y de la seguridad en las organizaciones*”. [en línea] [fecha de consulta: 6 de septiembre de 2023]. Disponible

en: https://www.segurilatam.com/tecnologias-y-servicios/ciberseguridad/la-importancia-del-ciberespacio-y-de-la-ciberseguridad-en-las-organizaciones_20200831.html.

- ACURIO DEL PINO, Santiago. “*Delitos Informáticos: Generalidades.*” [en línea] [fecha de Consulta: el 27 de septiembre de 2023]. Disponible en: https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf.
- CORONA, Pablo. “¿Qué es el ciberbullying?” [en línea] [fecha de consulta: 10 de septiembre de 2023]. Disponible en: <https://www.gob.mx/ciberbullying/articulos/que-es-el-ciberbullying>.
- DE LA CUESTA AGUADO, Paz, *Tipicidad e Imputación Objetiva*, extracto del artículo publicado en La imputación objetiva en el Derecho penal de Claus ROXIN, Editorial IDEMSA, Lima (Perú) 1997.
- ECHEVARRIA ROMERO, Luis Miguel. “*Marco conceptual de los delitos informáticos.*” Maestría computación e informática, Universidad Mayor de San Marcos, Lima- Perú, 2005.
- FANJUL FERNÁNDEZ, María Luisa. “*Conceptualización, evolución y clasificación del ciberdelito empresarial. Definición del ciberdelincuente. Implicaciones estratégicas.*” Madrid: AMEC Ediciones, 2018. ISBN 978-84-946590-5-8.
- FERRERAS FUENTE, Oliver. “*Ciberdelitos. El delio de Intrusismo informático en el ordenamiento jurídico español.*” [En línea]. Universidad de León [Fecha de Consulta: 08 de junio del 2023]. Disponible en: <https://buleria.unileon.es/bitstream/handle/10612/11363/Fuente%20Ferrer%20de%20la.pdf;jsessionid=571334418EEAD46F484CFEB1C01CADF2?sequence=1>.
- FERNÁNDEZ RODRÍGUEZ, Jose Julio. J. Los datos de tráfico de comunicaciones: En búsqueda de un adecuado régimen jurídico que elimine el riesgo de control permanente. *Revista Española de Derecho Constitucional* [en línea]. 2016, No. 108,

93-122. [fecha de consulta: 01 de mayo del 2023]. ISSN-L: 0211-5743 Disponible en: <http://dx.doi.org/10.18042/cepc/redc.108.03>.

- GONZÁLEZ LÓPEZ, Juan José. “La retención de datos de tráfico de las comunicaciones en la Unión Europea: una aproximación crítica” (en línea]. Editorial LA LEY. Universidad de Burgos. 15/12/2017. [fecha de consulta: 27 de marzo del 2023]. Disponible en : https://www.ubu.es/sites/default/files/portal_page/files/la_retencion_de_datos_de_trafico_de_las_comunicac..pdf.
- GONZALEZ QUEBEDO, Josefina. “*Investigación y prueba del cibercrimin*”. Tesis Doctoral Inédita, Universidad de Barcelona, 2017.
- LOPEZ, Jesica, FIGUEROA SÁENZ, Mónica. “*La Obtención De La Prueba Penal Internacional En Materia De Delitos Cibernéticos*” [en línea]. Monografía de grado para optar a título de abogado inédita, Universidad politécnico Gran Colombiano, Bogotá, 2018. [fecha de consulta: 27 de marzo del 2023]. Disponible en: <https://alejandria.poligran.edu.co/bitstream/handle/10823/1501/Cibercrimin%20%28Monica%20Senz%20-%20Jessica%20Lopez%29-Ultima%20version%20corregida.pdf?sequence=1&isAllowed=y>
- MIRO LLINARES, Fernando, delincuencia asociada al uso de las TIC, [en línea], Universidad abierta de Cataluña, España, 2013 [fecha de consulta: 25 de agosto del 2023]. Disponible en: <https://openaccess.uoc.edu/>.
- MUÑOZ CONDE, Francisco y GARCÍA ARAN, Mercedes, *Derecho Penal: Parte General*, 7ma Edición, Bogotá, Colombia, Ed. Tirant Lo Blanch, 2010.
- ORTS BERENGUER, Enrique y GONZÁLEZ CUSSAC, José, “**Manual de Derecho Penal. Parte General**”, proyecto de reforma y modernización normativa, CAJ/FIU-USAID, Managua, 2004.
- PALLADINO PELLÓN & Asociados Abogados Penalistas. “*¿Qué protege el Derecho penal El bien jurídico en el Derecho Penal?*” [en línea] [consultado el 8 de junio de

2023]. Disponible en: <https://www.palladinopellonabogados.com/el-bien-juridico-en-el-derecho-penal/>

- QUEZADA SALDAÑA, Martha Lorena. “*Análisis jurídico de la ley 1042: “Ley especial de ciberdelitos”*”. Managua, 2021.
- RODRÍGUEZ MADRIGAL, Bismarck, FLORES VASQUEZ, Fabio Ernesto, BERRIOS REYES, María Lissett. “*Los Delitos Informáticos y la Información como Nuevo Bien Jurídico Protegido*”. [en línea] León, junio 2006 [fecha de consulta: 1 de septiembre de 2023]. Disponible en: <http://riul.unanleon.edu.ni:8080/jspui/bitstream/123456789/1482/1/199275.pdf> .
- RAVENTOS PAJARES, Pepita. Los metadatos: que son y para qué sirven. *Revista d'arxiux* [en línea]. 2009, Núm. 8, P. 11 [fecha de consulta: 01 de mayo del 2023]. ISSN: 1696-1552. Disponible en: <http://arxiversvalencians.org/wp-content/uploads/2017/02/revista2009.pdf> .
- SAIN, Gustavo. Evolución Histórica de los delitos informáticos. *Revista pensamiento penal [en línea]*. 2015, abril [fecha de consulta: el 28 de abril del 2023]. ISSN: 1853-4554. Disponible en : [Evolución histórica de los delitos informáticos | Revista Pensamiento Penal](#).
- TIJERINO PACHECO, José María; COLOMER GOMEZ, Juan Luis; PELLENCER BARRIENTOS CRISOSTOMO, R. Cesar et.al. “*Manual de derecho procesal penal*”. 2ª ed. Valencia: TIRANT LO BLANCH, 2006. I.S.B.N.: 84 - 8456 - 549 -1.
- UNODC, “*Clasificación Internacional De Delitos Con Fines Estadísticos, versión 1.0*” [en línea]. Jonathan Gibbons ed. Vienna: marzo 2015. [fecha de consulta: 25 de agosto del 2023]. Disponible en: https://www.unodc.org/documents/data-and-analysis/statistics/crime/ICCS/ICCS_SPANISH_2016_web.pdf.
- VALDÉS, TÉLLEZ Julio. *Derecho informático*. 4ª ed. México, D.F: Mc Graw Hill Interamericana Editores, 2004. ISBN 9701043065

FUENTES TERCARIAS

Páginas web

- Real Academia Española. “*Diccionario de la lengua española*” [en línea] [fecha de consulta: el 31 de agosto del 2023]. Disponible en: <https://dle.rae.es/copyright?m=form>.
- Real Academia Española. “*Diccionario panhispánico del español jurídico*” [en línea] [fecha de consulta: 30 de agosto del año 2023]. Disponible en <https://dpej.rae.es/lema/delito-inform%C3%A1tico>.
- SoftwareLab.Org. “*¿Qué es el cibercrimen? La definición y los 5 tipos principales.*” [en línea] [fecha de Consulta: 08 de junio del 2023]. Disponible en [¿Qué es cibercrimen? La definición y los 5 tipos principales \(softwarelab.org\)](https://www.softwarelab.org/que-es-cibercrimen/).
- Avast Software s.r.o. “*¿Qué es una dirección IP?*” [en línea] [fecha de consulta: 11 de junio 2023]. Disponible en: <https://www.avast.com/es-es/c-what-is-an-ip-address>.
- Instituto De nutrición de Centro América Y Panamá [en línea] [fecha de Consulta: 19 de enero del 2023]. Disponible en: <http://www.incap.int/sisvan/index.php/es/acerca-de-san/797-sin-categoria/501-sistema-de-informacion>.
- *La Conservación De Datos Informáticos El Uso De Las Redes Internacionales 24/7 Y G/7 La Solicitud De Asistencia Judicial Internacional En El Marco De La Ciberdelincuencia*. Ministerio Público de Fiscalía de la Nación. Julio, No. 1. Lima, Perú: Unidad de cooperación judicial internacional y extradiciones, 2021. Disponible en <https://www.gob.pe/institucion/mpfn/informes-publicaciones/2116853-boletin-informativo-n-1-conservacion-de-datos-redes-internacionales-y-cooperacion-internacional>.
- Argentina Cibersegura. “*Ciberbullying ¿Qué es?*” [en línea] [fecha de consulta: 6 de septiembre de 2023]. Disponible en: https://www.argentinacibersegura.org/admin/resources/files/consejos/31/Guia_sobre_Cyberbullying.pdf

- ¿Qué es el sexting? - Tecnología - IntraMed. IntraMed [en línea]. [sin fecha] [consultado el 16 de febrero de 2023]. Disponible en: <https://www.intramed.net/contenidover.asp?contenidoid=93210>.
- ¿Qué es la "sextorsion"? - Noticias *IntraMed* [en línea]. [sin fecha] [consultado el 16 de febrero de 2023]. Disponible en: <https://www.intramed.net/contenidover.asp?contenidoid=93201>
- Grooming. *Argentina.gob.ar* [en línea]. [sin fecha] [consultado el 4 de octubre de 2023]. Disponible en: <https://www.argentina.gob.ar/grooming#:~:text=El%20GROOMING%20es%20la%20acción,chat%20o%20juegos%20en%20línea>.
- Stopbullyng.gob. “*Que es el ciberacoso.*” [en línea] [fecha de consulta: 16 de agosto del 2023]. <https://espanol.stopbullying.gov/acoso-por-internet-1yqc/qu%C3%A9-es> .
- ONU Women. “Prohibición de la discriminación, el acoso, incluido el acoso sexual, y el abuso de la autoridad” [en línea] [fecha de consulta: el 5 de octubre de 2023]. Disponible en: <https://www.un.org/womenwatch/uncoordination/antiharassment.html>
- Deep Traductor. [en línea] [fecha de consulta: 02 de diciembre del año 2023]. Disponible en: <https://www.deepl.com/es/translator#en/es/Global%20Commons>.
- *El perfil del usuario. Boletín UPIITA El camino a la innovación educativa*. No. 39. México. [en línea] [consultado el 6 de septiembre de 2023]. INSS 2007-6150. Disponible en: <http://www.boletin.upiita.ipn.mx/index.php/ciencia/510-cyt-numero-39/338-el-perfil-de-usuario>.
- CLARO COLOMBIA. [en línea] [fecha de Consulta: 6 de septiembre de 2023]. Disponible en: <https://www.claro.com.co/institucional/que-son-las-tic/>