

Memorando Nro. AN-CJEE-2021-0060-M

Quito, D.M., 01 de mayo de 2021

PARA: Sr. Mg. César Ernesto Litardo Caicedo
Presidente de la Asamblea Nacional

ASUNTO: Informe para Segundo Debate del "PROYECTO DE LEY ORGÁNICA REFORMATORIA DEL CÓDIGO ORGÁNICO INTEGRAL PENAL, PARA PREVENIR Y COMBATIR LA VIOLENCIA SEXUAL DIGITAL Y FORTALECER LA LUCHA CONTRA LOS DELITOS INFORMÁTICOS",

De mi consideración:

Con un corrial saludo, por disposición del Presidente de la Comisión Especializada Permanente de Justicia y Estructura del Estado, Dr. José Serrano Salgado, amparada en el artículo 56 de la Ley Orgánica Reformatoria de la Ley Orgánica de la Función Legislativa, remito a usted el Informe para Segundo Debate del "**PROYECTO DE LEY ORGÁNICA REFORMATORIA DEL CÓDIGO ORGÁNICO INTEGRAL PENAL, PARA PREVENIR Y COMBATIR LA VIOLENCIA SEXUAL DIGITAL Y FORTALECER LA LUCHA CONTRA LOS DELITOS INFORMÁTICOS**", aprobado por la Comisión Especializada Permanente de Justicia y Estructura del Estado, en la Sesión Virtual No. 165 realizada el día de ayer 30 de abril de 2021. De conformidad con la "Guía para Pocosos Legislativos durante la Emergencia Sanitaria" y al Memorando Nro. AN-SG-2020-0682-M de fecha 22 de mayo de 2020, suscrito por el Prosecretario General Temporal, adjunto el correo electrónico enviado por la Asambleísta Kharla Chávez Bajaña, confirmando su voto a favor del informe por cuanto no posee firma electrónica.

Con sentimientos de distinguida consideración.

Atentamente,

Documento firmado electrónicamente

Dra. Nathalia Veronica Jaramillo del Pozo
SECRETARIO RELATOR

Anexos:

- zimbra:_confirmacioñ_voto.pdf
- 1a30.04.2021_informe_segundo_debate_violencia_sexual_digital-signed(final).pdf

Copia:

Sr. Dr. José Ricardo Serrano Salgado
Presidente de la Comisión Especializada Permanente de Justicia y Estructura del Estado

Sr. Dr. Javier Aníbal Rubio Duque
Secretario General

ASAMBLEA NACIONAL DE LA REPÚBLICA DEL ECUADOR

**COMISIÓN ESPECIALIZADA PERMANENTE DE JUSTICIA
Y ESTRUCTURA DEL ESTADO**



**INFORME PARA SEGUNDO DEBATE DEL “PROYECTO DE LEY
ORGÁNICA REFORMATORIA DEL CÓDIGO ORGÁNICO INTEGRAL
PENAL, PARA PREVENIR Y COMBATIR LA VIOLENCIA SEXUAL
DIGITAL Y FORTALECER LA LUCHA CONTRA LOS DELITOS
INFORMÁTICOS”**

Integrantes:

José Ricardo Serrano Salgado, Presidente
Kharla del Rocío Chávez Bajaña, Vicepresidenta
Carlos Urel Ortega Álvarez
Henry Eduardo Cucalón Camacho
Luis Esteban Torres Cobo
María de Lourdes Cuesta Orellana
Elio Germán Peña Ontaneda
Rodrigo Collaguazo Pilco
Rosa Gina Orellana Román
Héctor Patricio Muñoz Alarcón
Franklin Omar Samaniego Maigua
Karla Gabriela Cadena Vélez

Quito, D.M., 30 de abril de 2021

CONTENIDO

1. OBJETO.....	5
2. ANTECEDENTES.....	5
3. PROCESO DE ELABORACIÓN DE INFORME PARA SEGUNDO DEBATE.....	9
3.1. Debate en el Pleno de la Asamblea Nacional.....	10
3.2. Sesiones de la Comisión.....	16
3.3. Asistencias de los miembros de la Comisión.....	17
3.4. Comisiones generales recibidas en las sesiones de la Comisión.....	18
4. ANÁLISIS Y RAZONAMIENTO.....	20
4.1. Observaciones recibidas por la Comisión.....	21
4.1.1. Sistematización y análisis de Observaciones.....	25
4.2. Temas incluidos para Segundo Debate.....	50
5. TECNOLOGÍA E INTERNET.....	50
5.1. Internet y la Sociedad: Éxitos y desafíos.....	52
5.2. Delitos informáticos: Características.....	54
5.3. Delitos en instituciones financieras u otras entidades.....	57
5.4. Principales derechos constitucionales reconocidos o vulnerados.....	59
5.5. Cooperación internacional.....	61
5.6. Responsabilidad proveedores de internet.....	62
5.7. Violencia Sexual Digital en América Latina y el Caribe.....	63
5.8. Violencia en línea contra las mujeres.....	65
5.9. Interseccionalidad.....	67
5.10. Sexualización del cuerpo de la mujer.....	68
5.11. Doble estándar.....	73
6. NORMATIVA INTERNACIONAL.....	76
6.1. Convención Americana sobre Derechos Humanos.....	76
6.2. Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer.....	77
6.3. Aplicación de recomendaciones efectuadas mediante la Observación General No. 25 sobre los derechos del niño en relación con el entorno digital	78
6.4. Adecuaciones para impulsar la Adhesión del Ecuador al Convenio de Budapest.....	79
7. DIFERENTES TIPOS DE VIOLENCIA EN EL ENTORNO DIGITAL.....	80
7.1. Grooming:.....	81
7.2. Mobbing y Bullying.....	84
7.3. Hostigamiento.....	86
7.4. Molestias virtuales.....	87
7.5. Ciberacoso sexual.....	87
7.6. Exposición a contenidos nocivos.....	88

7.7. Trasmisión en vivo/Streaming	88
7.8. Paliza feliz /Happy slapping.....	89
7.9. Sextorsión / Chantaje Sexual	90
7.10. Sexting no consentido / Violencia sexual digital	91
7.11. Deep fake porn	91
7.12. Creepshots	92
7.13. Doxing.....	92
7.14. Outing	93
7.15. Flaming	94
7.16. Sanciones propuestas en el COIP.....	94
8. DELITOS DE VIOLENCIA CONTRA LA MUJER O MIEMBROS DEL NÚCLEO FAMILIAR.....	97
8.1. Violencia económica y patrimonial	98
8.2. Violencia simbólica	99
8.3. Violencia política.....	100
8.4. Violencia mediática.....	101
8.5. Violencia gineco-obstétrica.....	102
8.6. Sanciones propuestas en el COIP.....	104
9. DELITOS INFORMÁTICOS	104
9.1. Phishing	104
9.2. Pharming	105
9.3. Cloning o skimming	106
9.4. Sanciones propuestas en el COIP.....	107
10. PROYECTO DE LEY ORGÁNICA REFORMATORIA DEL CÓDIGO ORGÁNICO INTEGRAL PENAL PARA PREVENIR Y COMBATIR LA VIOLENCIA SEXUAL DIGITAL Y FORTALECER LA LUCHA CONTRA LOS DELITOS INFORMÁTICOS..	108
11. RESOLUCIÓN.....	145
12. ASAMBLEÍSTA PONENTE	146
13. NOMBRE Y FIRMA DE LOS ASAMBLEÍSTAS QUE CONOCIERON Y SUSCRIBIERON EL INFORME	146
14. CERTIFICACIÓN:	148
15. BIBLIOGRAFÍA:	149

ÍNDICE DE TABLAS

Detalle:	Pág.
Tabla No. 1: OBSERVACIONES Y APORTES EN EL PLENO – PRIMER DEBATE.....	10
Tabla No. 2: SESIONES DE LA COMISIÓN.....	16
Tabla No. 3: ASISTENCIAS DE LOS MIEMBROS DE LA COMISIÓN.....	19
Tabla No. 4: COMISIONES GENERALES RECIBIDAS EN LA COMISIÓN.....	20
Tabla No. 5: OBSERVACIONES PRESENTADAS.....	21
Tabla No. 6: SISTEMATIZACIÓN DE OBSERVACIONES PRESENTADOS POR ESCRITO...25	
Tabla No. 7: TIPOS DE VIOLENCIA DIGITAL - Sanciones propuestas.....	94
Tabla No. 8: VIOLENCIA CONTRA LA MUJER - Sanciones propuestas.....	104
Tabla No. 9: DELITOS INFORMÁTICOS - Sanciones propuestas.....	107
Tabla No. 10: DETALLE DE LA VOTACIÓN.....	145

1. OBJETO.

Este documento tiene por objeto presentar el análisis realizado por los miembros de la Comisión Especializada Permanente de Justicia y Estructura del Estado, a las observaciones y aportes recibidas durante el tratamiento del “PROYECTO DE LEY ORGÁNICA REFORMATORIA DEL CÓDIGO ORGÁNICO INTEGRAL PENAL PARA PREVENIR Y COMBATIR LA VIOLENCIA SEXUAL DIGITAL Y FORTALECER LA LUCHA CONTRA LOS DELITOS INFORMÁTICOS”, a efectos de poner en conocimiento del Pleno de la Asamblea Nacional, el presente Informe para Segundo Debate elaborado por la Comisión.

2. ANTECEDENTES.

1. Mediante Oficio No. 292-2020-MMV-AN, de fecha 04 de agosto de 2020, ingresado en la Asamblea Nacional el mismo día, la Asambleísta Mae Montaña Valencia, presentó el “PROYECTO DE LEY ORGÁNICA PARA PREVENIR LA VIOLENCIA, EL ACOSO DIGITAL Y LA VIOLACIÓN A LA INTIMIDAD”;
2. Mediante Memorando Nro. AN-SMFO-2020-0043-M, de fecha 12 de agosto de 2020, ingresado en la Asamblea Nacional el mismo día, el Asambleísta Franklin Omar Samaniego Maigua, presentó el “PROYECTO DE LEY ORGÁNICA REFORMATORIA AL CÓDIGO ORGÁNICO INTEGRAL PENAL, PARA TIPIFICAR LOS DELITOS DE SEXTING Y HOSTIGAMIENTO”;
3. Mediante Memorando Nro. AN-SG-UT-2020-0116-M, de 13 de agosto de 2020, la Unidad de Técnica Legislativa a través del Informe No Vinculante No. 0125-INV-UTL-AN-2020 informa que el “PROYECTO DE LEY ORGÁNICA PARA PREVENIR LA VIOLENCIA, EL ACOSO DIGITAL Y LA VIOLACIÓN A LA INTIMIDAD”, cumple con los requisitos formales prescritos en los artículos 134 y 136 de la Constitución de la República; y, 54 y 56 de la Ley Orgánica de la Función Legislativa;

4. Mediante Memorando Nro. AN-SG-UT-2020-0127-M, de 24 de agosto de 2020, la Unidad de Técnica Legislativa a través del Informe No Vinculante No. 130-INV-UTL-AN-2020, informa que el “PROYECTO DE LEY ORGÁNICA REFORMATORIA AL CÓDIGO ORGÁNICO INTEGRAL PENAL, PARA TIPIFICAR LOS DELITOS DE SEXTING Y HOSTIGAMIENTO”, cumple con los requisitos formales prescritos en los artículos 134 y 136 de la Constitución de la República; y, 54 y 56 de la Ley Orgánica de la Función Legislativa;
5. Por medio de la Resolución CAL-2019-2021-325, suscrita el 01 de septiembre de 2020, el Consejo de Administración Legislativa, máximo órgano de administración legislativa resuelve calificar el “PROYECTO DE LEY ORGÁNICA REFORMATORIA AL CÓDIGO ORGÁNICO INTEGRAL PENAL, PARA TIPIFICAR LOS DELITOS DE SEXTING Y HOSTIGAMIENTO”, en virtud de que cumple con todos los requisitos establecidos en la Constitución y en la Ley, por lo que, remite dicho Proyecto de Ley a la Comisión Especializada Permanente de Justicia y Estructura del Estado, a fin de que inicie su tramitación; y, para que de ser el caso, lo unifique con los demás proyectos que correspondan a la misma materia.
6. Por medio de la Resolución CAL-2019-2021-327, suscrita el 01 de septiembre de 2020, el Consejo de Administración Legislativa, máximo órgano de administración legislativa resuelve calificar el “PROYECTO DE LEY ORGÁNICA PARA PREVENIR LA VIOLENCIA, EL ACOSO DIGITAL Y LA VIOLACIÓN A LA INTIMIDAD”, en virtud de que cumple con todos los requisitos establecidos en la Constitución y en la Ley, por lo que, remite dicho Proyecto de Ley a la Comisión Especializada Permanente de Justicia y Estructura del Estado, a fin de que inicie su tramitación; y, para que de ser el caso, lo unifique con los demás proyectos que correspondan a la misma materia.
7. Mediante Sesión Virtual No. AN-CEPJEE-2019-2021-116, de 30 de septiembre de 2020, la Comisión Especializada Permanente de Justicia y Estructura del Estado, avoca conocimiento de la Resolución CAL-2019-2021-325, suscrita el 01 de septiembre de 2020, que califica el referido

- “PROYECTO DE LEY ORGÁNICA REFORMATORIA AL CÓDIGO ORGÁNICO INTEGRAL PENAL, PARA TIPIFICAR LOS DELITOS DE SEXTING Y HOSTIGAMIENTO”, que ha sido remitida a esta Comisión para que inicie su tratamiento y que de ser el caso, se los unifique con los demás proyectos que correspondan a la misma materia.
8. Mediante Sesión Virtual No. AN-CEPJEE-2019-2021-118, de 19 de octubre del 2020, la Comisión Especializada Permanente de la Comisión de Justicia y Estructura del Estado, avoca conocimiento de la Resolución CAL-2019-2021-327, suscrita el 01 de septiembre de 2020, que califica el referido “PROYECTO DE LEY ORGÁNICA PARA PREVENIR LA VIOLENCIA, EL ACOSO DIGITAL Y LA VIOLACIÓN A LA INTIMIDAD”, que ha sido remitida a esta Comisión para que inicie su tratamiento y que de ser el caso, se los unifique con los demás proyectos que correspondan a la misma materia.
 9. En Sesión Virtual No. AN-CEPJEE-2019-2021-140, de 13 de enero de 2021, la Comisión Especializada Permanente de Justicia y Estructura del Estado, recibió en Comisión General a la Asambleísta Mae Montaña, ponente del “PROYECTO DE LEY ORGÁNICA PARA PREVENIR LA VIOLENCIA, EL ACOSO DIGITAL Y LA VIOLACIÓN A LA INTIMIDAD”.
 10. En Sesión Virtual No. AN-CEPJEE-2019-2021-146, de 10 de febrero de 2020, la Comisión Especializada Permanente, recibió en Comisión General al Asambleísta Franklin Samaniego, ponente del “PROYECTO DE LEY ORGÁNICA REFORMATORIA AL CÓDIGO ORGÁNICO INTEGRAL PENAL, PARA TIPIFICAR LOS DELITOS DE SEXTING Y HOSTIGAMIENTO”.
 11. En Sesión Virtual No. AN-CEPJEE-2019-2021-146, de fecha 10 de febrero de 2021, la Comisión Especializada Permanente de Justicia y Estructura del Estado, por cuanto los referidos proyectos de Ley versan sobre reformas al Código Orgánico Integral Penal en materia de violencia sexual digital, resolvió por unanimidad unificar estos dos referidos proyectos de Ley en el “PROYECTO DE LEY ORGÁNICA REFORMATORIA DEL CÓDIGO ORGÁNICO INTEGRAL PENAL Y DE

LA LEY ORGÁNICA INTEGRAL PARA PREVENIR Y ERRADICAR LA VIOLENCIA CONTRA LAS MUJERES, PARA PREVENIR Y SANCIONAR LA VIOLENCIA SEXUAL DIGITAL”.

12. La Comisión Especializada Permanente de Justicia y Estructura del Estado, en sesiones virtuales números: AN-CEPJEE-2019-2021-140, de 13 de enero de 2021; AN-CEPJEE-2019-2021-144, de 01 de febrero de 2021; AN-CEPJEE-2019-2021-146, de 10 de febrero de 2021; AN-CEPJEE-2019-2021-148, de 23 de febrero de 2021; AN-CEPJEE-2019-2021-151, de 08 de marzo de 2021; AN-CEPJEE-2019-2021-153, de 12 de marzo de 2021; AN-CEPJEE-2019-2021-154, de 15 de marzo de 2021; y, AN-CEPJEE-2019-2021-157, de 24 de marzo de 2021, recibió en Comisión General a diversos expertos y académicos nacionales e internacionales, así como también, a autoridades de diferentes entidades públicas que han presentado sus observaciones y aportes al “PROYECTO DE LEY ORGÁNICA REFORMATORIA DEL CÓDIGO ORGÁNICO INTEGRAL PENAL Y DE LA LEY ORGÁNICA INTEGRAL PARA PREVENIR Y ERRADICAR LA VIOLENCIA CONTRA LAS MUJERES, PARA PREVENIR Y SANCIONAR LA VIOLENCIA SEXUAL DIGITAL”.

13. La Comisión Especializada Permanente de Justicia y Estructura del Estado, en sesión virtual No. AN-CEPJEE-2019-2021-160, de 29 de marzo de 2021; revisó los insumos y avances del equipo técnico, y avanzó con el análisis y tratamiento para Primer Debate del “PROYECTO DE LEY ORGÁNICA REFORMATORIA DEL CÓDIGO ORGÁNICO INTEGRAL PENAL Y DE LA LEY ORGÁNICA INTEGRAL PARA PREVENIR Y ERRADICAR LA VIOLENCIA CONTRA LAS MUJERES, PARA PREVENIR Y SANCIONAR LA VIOLENCIA SEXUAL DIGITAL”.

14. La Comisión Especializada Permanente de Justicia y Estructura del Estado, en sesión virtual No. AN-CEPJEE-2019-2021-160, de 29 de marzo de 2021; revisó los insumos y avances del equipo técnico, y avanzó con el análisis y tratamiento para Primer Debate del “PROYECTO DE LEY ORGÁNICA REFORMATORIA DEL CÓDIGO ORGÁNICO INTEGRAL PENAL Y DE LA LEY ORGÁNICA INTEGRAL PARA PREVENIR Y

ERRADICAR LA VIOLENCIA CONTRA LAS MUJERES, PARA PREVENIR Y SANCIONAR LA VIOLENCIA SEXUAL DIGITAL”.

15. Con fecha 06 de abril de 2021, mediante Sesión No. 699 en modalidad virtual del Pleno de la Asamblea Nacional, se desarrolló el Primer Debate del referido proyecto de Ley.
16. En sesiones virtuales de Comisión No. AN-CEPJEE-2019-2021-162; y, AN-CEPJEE-2019-2021-163, de fechas 14 y 23 de abril de 2021, respectivamente, los asambleístas miembros de la Comisión conocieron y analizaron las observaciones y aportes realizados en el Primer Debate del Pleno de la Asamblea Nacional, dentro del proyecto de Ley en tratamiento.
17. Finalmente, con fecha 30 de abril de 2021, en sesión virtual No. AN-CEPJEE-2019-2021-165, el Pleno de la Comisión Especializada Permanente de Justicia y Estructura del Estado, APRUEBA por unanimidad el Informe para Segundo Debate del “PROYECTO DE LEY ORGÁNICA REFORMATORIA DEL CÓDIGO ORGÁNICO INTEGRAL PENAL PARA PREVENIR Y COMBATIR LA VIOLENCIA SEXUAL DIGITAL Y FORTALECER LA LUCHA CONTRA LOS DELITOS INFORMÁTICOS” y lo remitió al Presidente de la Asamblea Nacional, a fin de que el Pleno de este parlamento sea convocado a Segundo Debate.

3. PROCESO DE ELABORACIÓN DE INFORME PARA SEGUNDO DEBATE.

En esta sección, se resume el proceso de análisis y estudio que sirvió de base para la elaboración del presente Informe para Segundo Debate.

Tras el análisis de los temas realizado al interior de la Comisión de Justicia y Estructura del Estado y luego de las múltiples comparecencias de expertos nacionales e internacionales recibidas; y, por cuanto el presente Proyecto de Ley versa sobre dos grandes ejes, se ha considerado pertinente modificar la

denominación del mismo¹, con el fin de abarcar tanto a Violencia Sexual Digital, como a Delitos Informáticos, haciendo énfasis en la prevención y combate a todo tipo de violencia en el entorno digital, así como al fortalecimiento de la lucha contra los delitos informáticos.

3.1. Debate en el Pleno de la Asamblea Nacional.

En el desarrollo del Primer Debate del “PROYECTO DE LEY ORGÁNICA REFORMATORIA DEL CÓDIGO ORGÁNICO INTEGRAL PENAL PARA PREVENIR Y COMBATIR LA VIOLENCIA SEXUAL DIGITAL Y FORTALECER LA LUCHA CONTRA LOS DELITOS INFORMÁTICOS”, en el Pleno de la Asamblea Nacional, se contó con la intervención de Isabella Nuques², a quien se la recibió en Comisión General; y siete legisladores³, quienes presentaron sus observaciones y aportes a este proyecto de Ley en análisis y tratamiento dentro de la Comisión, conforme se detalla a continuación:

Tabla N° 1

OBSERVACIONES Y APORTES EN EL PLENO – PRIMER DEBATE

Nro.	PROPONENTE	ART.	PROPUESTA U OBSERVACIÓN
1	Isabella Nuques, Activista y víctima de porno venganza y ciberacoso	Ciberacoso sexual	Aumentar los años de pena, las sentencias mínimas deberían de ser de 5 a 7 años y con agravantes de 7 a 13 años.
2		Violencia de Género	La violencia sexual digital debería ser tratado y estipulado en la Ley como “ <i>violencia de género</i> ”.

¹ El “Proyecto de Ley Orgánica para Prevenir la Violencia, al Acoso Digital y la Violación a la Intimidad”, presentado por la Asambleísta Mae Montaña; y, el “Proyecto de Ley Orgánica Reformatoria al Código Orgánico Integral Penal, para tipificar los delitos de Sexting y Hostigamiento” presentado por el Asambleísta Franklin Omar Samaniego Maigua, fueron unificados como “Proyecto de Ley Orgánica Reformatoria del Código Orgánico Integral Penal y de la Ley Orgánica Integral para Prevenir y Erradicar la Violencia Contra las Mujeres, para Prevenir y Sancionar la Violencia Sexual Digital”, y actualmente quedó denominada como “**Proyecto de Ley Orgánica Reformatoria del Código Orgánico Integral Penal para Prevenir y Combatir la Violencia Sexual Digital y Fortalecer la Lucha Contra los Delitos Informáticos**”.

² Activista y víctima de porno venganza y ciberacoso, quien dio a conocer su testimonio frente al Pleno de la Asamblea Nacional.

³ As. José Serrano Salgado, Presidente de la Comisión Especializada Permanente de Justicia y Estructura del Estado; As. Héctor Muñoz; As. Henry Cucalón; As. Franklin Samaniego; As. Esteban Torres; As. Mae Montaña; y, As. Dallyana Passailaigue.

3		Prisión preventiva	Si el presunto agresor es capturado en delito flagrante solo debe tener la opción de prisión preventiva hasta finalizar el proceso judicial así se respalda a la víctima y su integridad, evitando de nuevo ser perjudicada en las redes.	
4		Extorsión sexual	La sextorsión debería ser añadida, ya que ahora es muy común y existen grupos de mafia que piden dinero para no difundir material sexual. Incluir este delito como agravante en el art.185 del COIP sobre extorsión.	
5		Violencia Digital	Los casos de violencia digital deberían ser ágiles y no durar más de 6 meses.	
6		Eliminación de material difundido en redes	Se debería tratar de eliminar el material expuesto en redes lo más pronto posible luego de los peritajes.	
7		Personal especializado	Deben existir policías, peritos, ficales y jueces expertos en este tema y ser afines a casos de violencia de género para evitar la revictimización.	
8		Herramientas y entrenamientos claves	Los policías deben tener las herramientas y entrenamientos claves para que los casos no se caigan.	
9		Cooperación entre Fiscalía y plataformas digitales	Resaltar el apoyo que debe tener Fiscalía para agilizar las investigaciones y nexos con las plataformas digitales mundialmente.	
10		Otras formas de violencia digital	Se deben analizar más tipos de violencia digital: <i>doxing</i> , <i>cyberstalking</i> , ciberacoso, violencia digital, la creación de perfiles falsos a nombre de la víctima, sextorsión, <i>deepfake porn</i> .	
11		As. Héctor Muñoz	Campañas de Sensibilización	Deben implementarse campañas de sensibilización y capacitación a nivel nacional como medida de prevención

			para que se conozca como proceder ante estos delitos.
12		Campañas de difusión sobre la violencia sexual digital	Es imperante la necesidad de campañas de difusión nacional sobre los derechos vulnerados y sus consecuencias, en virtud de que estos factores acarrear graves repercusiones en la salud mental y terminan convirtiéndose en una alarma de salud pública.
13		Fortalecimiento de la educación en materia de violencia sexual digital	Señala que la educación es una herramienta fundamental para erradicar la normalización de la violencia de género.
14	As. Henry Cucalón	Extorsión sexual	Se debe contar con un proyecto de Ley más amplio, con conductas invisibilizadas o normalizadas, como la sextorsión.
15		Ciberacoso sexual Divulgación de contenido sexual explícito sin consentimiento	Al definir el ciberacoso sexual y divulgación de contenido sexual explícito sin consentimiento, se habla de “medios tecnológicos presentes o futuros”, sugiere eliminar esta frase.
16		Divulgación de contenido sexual explícito sin consentimiento	Respecto a la inhabilitación al acceso a medios digitales, cuestiona la dificultad de aplicar esta norma.
17		Divulgación de contenido sexual explícito sin consentimiento	Según el articulado, solo se podrá sancionar el delito de divulgación cuando esta cause daño, perjuicio o afecte ciertos derechos, esto haría una norma ineficaz, ya que impone requisitos pre procesales que limitarían el proceso, por consiguiente, esta situación devendría inclusive en un caso civil para probar dichos hechos.
18		Aclaración	Se necesita aclarar en la norma el tema relativo al tipo de imágenes que

			se puedan utilizar para presentaciones profesionales.
19		Ataque a la integridad de sistemas informáticos	No es conveniente eliminar el último inciso del articulado ya que se estaría eliminando el agravante ante bienes de primera necesidad.
20		Obtención de Prueba por Medio de Cooperación Internacional	Con respecto a la inclusión de la Sección Quinta en el COIP, será el fiscal quien tenga tales atribuciones, por ende, sería legislar muy amplio y podría resultar inaplicable.
21	As. Franklin Samaniego	Proteger la dignidad de las personas	Se necesita ciberseguridad, políticas públicas, protocolos de violencia, proteger la dignidad de las personas y proyecto de vida.
22		Hostigamiento	Se debería tipificar la conducta dolosa de hostigar en todos los espacios de la vida, que afecta a la libertad de las personas y proyecto de vida. No necesariamente vinculada con la necesidad sexual.
23		Procesamiento de datos y demás procedimientos	Debe aclararse que la atribución debe ser del juez mas no del fiscal.
24		Cooperación internacional	Es importante que todos los convenios que se vayan a ratificar pasen por el respectivo control de constitucionalidad. Debe incluirse esto en el articulado.
25	As. Esteban Torres	Estructura del proyecto de Ley	Debe mejorarse la estructura del proyecto, ya que solo se reforman 3 artículos sobre violencia sexual digital y 7 sobre ciberseguridad.
26		Ciberacoso sexual	Este artículo debería Incluirse a continuación del acoso sexual. Se debe analizar si es necesario un nuevo artículo o a su vez, solo incluir un párrafo final dentro del mismo Art. 166.

27	Ciberacoso sexual Divulgación de contenido sexual explícito sin consentimiento	La expresión “ <i>medios tecnológicos presentes o futuros</i> ”, es cuestionable, ya que al momento que un algoritmo hace daño ya se hace presente.
28	Ciberacoso sexual	Se incluyen 9 verbos rectores, que no dan claridad al artículo, además, no es directo respecto a “ <i>incitar</i> ”. La fuerza ya está dentro del Art. 166. Solo debe incluirse la siguiente frase “ <i>por medios digitales o telemáticos.</i> ”
29	Ciberacoso sexual	Resultaría innecesario, porque ya todos los verbos rectores llevan implícito que se esté generando algún tipo de daño.
30	Ciberacoso sexual	La inhabilitación a medios digitales sería absolutamente inaplicable.
31	Ciberacoso sexual	No se entiende qué es revictimización, tampoco los límites en la investigación y la revictimización.
32	Divulgación de contenido sexual explícito sin consentimiento	El artículo precedente se refiere ya a la violación a la intimidad. Debe definirse si hace falta crear este nuevo artículo o solo aumentarlo como un párrafo dentro del mismo Art. 178.
33	Divulgación de contenido sexual explícito sin consentimiento	La acción de “ <i>viralizar</i> ”, conlleva a muchas personas, más no solo a una, el término no sería técnico y está fuera de la responsabilidad de una persona.
34	Divulgación de contenido sexual explícito sin consentimiento	Las acciones de “ <i>Divulgar</i> ” o “ <i>publicar</i> ” se repetirían con el Art. 178.
35	Divulgación de contenido sexual explícito	La ausencia de consentimiento de la víctima ya se encuentra en el Art. 178. Es importante resaltar la

		sin consentimiento	inclusión “ <i>causar daño</i> ”; eso está correcto.
36		Divulgación de contenido sexual explícito sin consentimiento	No se entiende claramente la disposición respecto a “ <i>dispositivo electrónico que no sea de propiedad del infractor, sea que este haya sido encontrado, perdido, robado o hurtado previamente.</i> ”
37		Divulgación de contenido sexual explícito sin consentimiento	Resalta la comercialización, como “ <i>only fans</i> ” donde alguien podría pagar para tener acceso, y esa información divulgarla sin autorización.
38		Divulgación de contenido sexual explícito sin consentimiento	La inhabilitación de acceso a medios digitales no se entiende, resultaría inaplicable.
39		Estructura del proyecto de Ley	Resalta la tipificación de artículos sobre delitos de ciberseguridad, pero insiste en que debe revisarse la necesidad o no de inclusión como nuevos artículos o ajustes técnicos a artículos ya existentes.
40	As. Mae Montaña	Divulgación de contenido sexual explícito sin consentimiento	Debe tomarse en cuenta que la divulgación de contenido se da cuando el que recibe la imagen o contenido es un par, porque no siempre son delincuentes, sino también los jóvenes son víctimas y victimarios.
41		Extorsión sexual	Al tipificarse el delito, debe diferenciarse y enfatizarse la sextorsión de una simple extorsión genérica para que no quepa duda al momento de aplicar la norma por parte de los administradores de justicia, en esos casos brilla la impunidad.
42		Medidas correctivas	Quien comete un delito, debe tener medidas correctivas acorde al grado de gravedad del perjuicio causado.

43	Porno venganza y comercialización de contenido íntimo o personal	No es lo mismo la “porno venganza” y la “comercialización de este contenido”, deben ser considerados como agravantes.
44	Fortalecimiento de la educación	Debe enseñarse estos temas a los estudiantes como medida preventiva y disuasiva, tanto en escuelas, colegios y universidades.

3.2. Sesiones de la Comisión.

De la misma manera, es importante señalar las sesiones que ha llevado a cabo la Comisión de Justicia y Estructura del Estado, a efectos de elaborar el presente Informe para Segundo Debate, conforme se detalla a continuación:

Tabla N° 2
SESIONES DE LA COMISIÓN

FECHA	CONV.	SESIÓN	ORDEN DEL DÍA
14.04.2021	374	162	<p>1.- Dentro del marco del tratamiento para el Segundo Debate del “PROYECTO DE LEY ORGÁNICA REFORMATORIA DEL CÓDIGO ORGÁNICO INTEGRAL PENAL Y DE LA LEY ORGÁNICA INTEGRAL PARA PREVENIR Y ERRADICAR LA VIOLENCIA CONTRA LAS MUJERES, PARA PREVENIR Y SANCIONAR LA VIOLENCIA SEXUAL DIGITAL”:</p> <p>a. Recibir en Comisión General a Alexandra Guerrón especialista en erradicación de violencia ONU MUJERES ECUADOR.</p> <p>b. Recibir en Comisión General al Dr. José Luis Barzallo, experto en derecho de las nuevas tecnologías de la información y las telecomunicaciones.</p> <p>c. Recibir en Comisión General a Claire Lee PHD de la Universidad de Singapur, Profesora de la</p>

			<p>Escuela de Criminología y Estudios de Justicia en Universidad de Massachusetts, experta en Ciberdelincuencia, Ciberseguridad, <i>Big Data</i>, Criminología comparada, Sociología. (Se excusa)</p> <p>d. Recibir en Comisión General a la Asambleísta Wilma Andrade Muñoz, quien hará una exposición sobre la propuesta planteada.</p>
23.04.2021	375	163	<p>2.- Dentro del marco del tratamiento para el Segundo Debate del “PROYECTO DE LEY ORGÁNICA REFORMATORIA DEL CÓDIGO ORGÁNICO INTEGRAL PENAL Y DE LA LEY ORGÁNICA INTEGRAL PARA PREVENIR Y ERRADICAR LA VIOLENCIA CONTRA LAS MUJERES, PARA PREVENIR Y SANCIONAR LA VIOLENCIA SEXUAL DIGITAL”:</p> <p>a. Recibir en Comisión General a la Doctora Virginia Gómez de la Torre, Directora de la Fundación Desafío Coalición Nacional de Mujeres del Ecuador.</p> <p>b. Recibir en Comisión General a Ana Cristina Vea Sánchez, Directora Ejecutiva del Centro de Apoyo y Protección de los Derechos Humanos, Surkuna.</p>

Fuente: Secretaría de la Comisión Especializada Permanente de Justicia y Estructura del Estado.

3.3. Asistencias de los miembros de la Comisión.

La Tabla 3 resume las sesiones de la Comisión y asistencias de los señores legisladores a las mismas, luego de cerrado el Primer Debate en el Pleno de la Asamblea Nacional, con el fin de analizar y debatir las observaciones y aportes al referido “PROYECTO DE LEY ORGÁNICA REFORMATORIA DEL CÓDIGO ORGÁNICO INTEGRAL PENAL PARA PREVENIR Y COMBATIR LA VIOLENCIA SEXUAL DIGITAL Y FORTALECER LA LUCHA CONTRA LOS DELITOS INFORMÁTICOS”.

Tabla No. 3
ASISTENCIAS DE LOS MIEMBROS DE LA COMISIÓN

CONVOCATORIA	320	322	348	352	355	357	361	363	364	368	368	371	374	375	377	TOTAL ASISTENCIA
SESIÓN	116	118	140	144	146	148	151	153	154	157	Cont. 157	160	162	163	165	
FECHA	30.09.2020	19.10.2020	13.01.2021	01.02.2021	10.02.2021	23.02.2021	08.03.2021	12.03.2021	15.03.2021	24.03.2021 10H00	24.03.2021 15H30	29.03.2021	14.04.2021	23.04.2021	30.04.2021	
ASAMBLEÍSTA	REFERENCIA: P = Presente; AL = Asiste alterno; A = Ausente; AJ = Ausente justificación.															
As. José Ricardo Serrano	P	P	P	P	P	A	P	P	P	P	P	P	P	P	P	Asistencias: 14 Alterno: 0 Ausencias: 1
As. Kharla Chávez	P	P	P	P	P	P	P	AL	AL	A	P	P	AL	P	P	Asistencias: 11 Alterno: 3 Ausencias: 1
As. Carlos Ortega	N/A	P	P	P	P	P	P	P	P	P	P	P	P	P	P	Asistencias: 14 Alterno: 0 Ausencias: 0
As. Henry Cucalón	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	Asistencias: 15 Alterno: 0 Ausencias: 0
As. Esteban Torres	P	P	AL	AL	P	P	P	P	P	P	P	P	P	P	P	Asistencias: 13 Alterno: 2 Ausencias: 0
As. Lourdes Cuesta	P	P	AL	AL	P	P	P	P	P	P	P	P	P	P	P	Asistencias: 13 Alterno: 2 Ausencias: 0
As. Elio Peña	P	P	P	P	P	P	P	P	P	P	AJ	P	AJ	P	P	Asistencias: 13 Alterno: 0 Ausencias: 2
As. Rodrigo Collaguazo	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	Asistencias: 15 Alterno: 0 Ausencias: 0
As. Rosa Orellana	P	P	AL	AL	P	P	P	P	P	P	P	P	P	P	P	Asistencias: 13 Alterno: 2 Ausencias: 0
As. Héctor Muñoz	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	Asistencias: 15 Alterno: 0 Ausencias: 0
As. Franklin Samaniego	P	P	AL	AL	P	P	P	P	P	P	P	P	P	P	P	Asistencias: 13 Alterno: 2 Ausencias: 0
As. Karla Cadena	AJ	P	P	P	P	P	P	P	P	P	P	P	AJ	P	P	Asistencias: 13 Alterno: 0 Ausencias: 2
As. Ximena Peña	P	N/A	N/A	N/A	N/A	N/A	N/A	Asistencias: 1 Alterno: 0 Ausencias: 0								
Total:	12	12	12	12	12	11	12	12	12	11	12	12	11	12	12	

Fuente: Secretaría de la Comisión Especializada Permanente de Justicia y Estructura del Estado.

3.4. Comisiones generales recibidas en las sesiones de la Comisión.

La Tabla 4 resume las comisiones generales recibidas en las sesiones de la Comisión, para analizar y debatir las observaciones y aportes al referido “PROYECTO DE LEY ORGÁNICA REFORMATORIA DEL CÓDIGO ORGÁNICO INTEGRAL PENAL EN MATERIA ANTICORRUPCIÓN”.

Tabla No. 4

COMISIONES GENERALES RECIBIDAS EN LA COMISIÓN

FECHA	CONV.	SESIÓN	COMISIONADO/A	TEMA
14.04.2021	374	162	As. Wilma Andrade, Asambleísta Nacional	Presenta su propuesta de despenalización del aborto ⁴ para casos de violación, dentro del presente paquete de reformas al COIP que se está analizando en esta Comisión.
			Dra. Alexandra Guerrón, Especialista en erradicación de violencia ONU MUJERES ECUADOR.	Presenta sus observaciones y aportes al "PROYECTO DE LEY ORGÁNICA REFORMATORIA DEL CÓDIGO ORGÁNICO INTEGRAL PENAL Y DE LA LEY ORGÁNICA INTEGRAL PARA PREVENIR Y ERRADICAR LA VIOLENCIA CONTRA LAS MUJERES, PARA PREVENIR Y SANCIONAR LA VIOLENCIA SEXUAL DIGITAL".

⁴ En este sentido, Ecuador obtiene un nuevo logro en su lucha por los derechos de las mujeres al permitir la interrupción voluntaria del embarazo en casos de violación sexual. Este 28 de abril de 2021 se acaba de convertir en un día histórico para Ecuador, pues la Corte Constitucional acaba de despenalizar el aborto por violación con siete votos a favor y dos en contra, resolviendo en torno a siete demandas de inconstitucionalidad planteadas por organizaciones feministas, de derechos humanos y Defensoría del Pueblo. De esta manera, han dado paso a la inconstitucionalidad de los artículos 149 y 150 del Código Orgánico Integral Penal, sin embargo, aún se espera algún pronunciamiento oficial por parte de este organismo y de la notificación del respectivo fallo constitucional, en calidad de máximo organismo de interpretación constitucional en el país. Varias posturas se han presentado, tanto a favor como en contra de la despenalización del aborto en casos de violación, por un lado, acogieron con satisfacción el fallo, considerando que *"La Corte Constitucional este día actuó como un organismo técnico, que debe interpretar leyes y derechos. Era urgente y era lo mínimo, porque las sobrevivientes de violencia sexual deben poder decidir abortar sin verse en riesgo de ser encarceladas o de recurrir a abortos inseguros en la clandestinidad"* (Foro por la Salud Pública. Entrevista Diario El Comercio), asimismo, manifestaron que: *"Hay una enorme diferencia entre legalizar el aborto y despenalizar el aborto en casos de violación. Es irresponsable confundir una y otra cuestión, para fortalecer posturas medievales."* (Abg. María Dolores Miño, Especialista en Derechos Humanos con experiencia en litigio ante el Sistema Interamericano, defensa y promoción de Derechos Humanos desde la sociedad civil, desarrollo de políticas públicas desde el sector público y docencia universitaria. Pronunciamiento vía Twitter.) Por otro lado, desde espacios como la Conferencia Episcopal Ecuatoriana enviaron una carta al Dr. Hernán Salgado, Presidente de la Corte Constitucional, expresando su preocupación sobre el tema y en la que rechazan la despenalización del aborto por violación desde el ente de justicia, señalando que: *"Amparados en la Constitución Política del Ecuador y en las normas internacionales suscritas y ratificadas por nuestra nación, apelamos a la conciencia de los Honorables Magistrados de la Corte Constitucional, para que en este momento histórico de mayor sensibilidad hacia lo auténticamente humano sepan marcar una pauta de acción ética, humana y solidaria, a través de sus decisiones"*.

			<p>Dr. José Luis Barzallo, Experto en derecho de las nuevas tecnologías de la información y las telecomunicaciones.</p>	<p>Presenta sus observaciones y aportes al “PROYECTO DE LEY ORGÁNICA REFORMATORIA DEL CÓDIGO ORGÁNICO INTEGRAL PENAL Y DE LA LEY ORGÁNICA INTEGRAL PARA PREVENIR Y ERRADICAR LA VIOLENCIA CONTRA LAS MUJERES, PARA PREVENIR Y SANCIONAR LA VIOLENCIA SEXUAL DIGITAL”.</p>
23.04.2021	375	163	<p>Dra. Virginia Gómez de la Torre, Directora de la Fundación Desafío Coalición Nacional de Mujeres del Ecuador.</p>	<p>Presentan argumentos en apoyo a la despenalización del aborto en casos de violación en el marco de la propuesta presentada por la As. Wilma Andrade.</p>
			<p>Dra. Ana Cristina Vera Sánchez, Directora Ejecutiva del Centro de Apoyo y Protección de los Derechos Humanos, Surkuna.</p>	<p>Presentan información actual y relevante que da cuenta de la realidad que viven las mujeres, niñas, adolescentes y personas con capacidad de gestar en relación con el ejercicio de sus derechos sexuales y derechos reproductivos y su acceso a la justicia; así como de la situación de violencia sexual y embarazos durante la pandemia y su relación con la insuficiente atención y acceso a los servicios de salud reproductiva.</p>

4. ANÁLISIS Y RAZONAMIENTO.

El presente análisis y razonamiento, responde a la discusión de los principales aspectos técnicos y jurídicos del proyecto de Ley y los argumentos que guiaron su discusión a lo largo de la construcción del presente informe, al interior de la Comisión.

4.1. Observaciones recibidas por la Comisión.

La Tabla 5 sistematiza las observaciones presentadas por los señores asambleístas e instituciones públicas, con respecto al “PROYECTO DE LEY ORGÁNICA REFORMATORIA DEL CÓDIGO ORGÁNICO INTEGRAL PENAL PARA PREVENIR Y COMBATIR LA VIOLENCIA SEXUAL DIGITAL Y FORTALECER LA LUCHA CONTRA LOS DELITOS INFORMÁTICOS”.

Tabla No. 5
OBSERVACIONES PRESENTADAS

No.	FECHA	OFICIO No.	REMITENTE	DETALLE	ARTICULOS OBSERVADOS
1	12.02.2021	Oficio No. 21-2021-SG	Centro Ecuatoriano para la Promoción y Acción de la Mujer — CEPAM	Observaciones y aportes al PROYECTO DE LEY ORGÁNICA REFORMATORIA AL CÓDIGO ORGÁNICO INTEGRAL PENAL, PARA TIPIFICAR LOS DELITOS DE "SEXTING"; Y, "HOSTIGAMIENTO"	1. Consideraciones generales. 2. Observaciones al Art. 163A. Hostigamiento. 3. Observaciones al Art. 179A.- <i>Sexting</i> .
2	09.03.2021	Oficio Nro. MREMH-MREMH-2021-0121-OF	Dr. Luis Benigno Gallegos Chiriboga, Ministro de Relaciones Exteriores y Movilidad Humana.	Estado actual de la posible adhesión al del Ecuador al Convenio de Budapest.	1. Remite Ayuda Memoria relativa al proceso de adhesión del Ecuador al Convenio de Budapest. 2. Informe de la Consultoría de "Glacy Plus" - Análisis de las posibles reformas que se requerirán para ajustar la legislación ecuatoriana al

					Convenio de Budapest.
3	24.03.2021	s/n	Dr. Francisco Ramiro Cevallos Tejada, Secretario Técnico Consejo Nacional para la Igualdad Intergeneracional	Informe al Proyecto de Ley Orgánica Reformatoria del Código Orgánico Integral Penal y de la Ley Orgánica Integral para Prevenir y Erradicar la Violencia Contra las Mujeres, para Prevenir y Sancionar la Violencia Sexual Digital	1. Observaciones al artículo de "Hostigamiento". 2. Observaciones al artículo de "Violencia sexual digital". 3. Observaciones al artículo de "Ciberacoso Sexual". 4. Observaciones al artículo de "Disposiciones comunes a los delitos de violencia sexual digital." 5. Observaciones al artículo de "Sexting". 6. Propone incluir luego del Art. 179, los siguientes artículos: a) Art. 179XX.- Violencia contra niñas, niños y adolescentes a través de tecnologías de la información y las comunicaciones b) Art. 179XX.- Grooming c) Art. 179XX.- Fleming d) Art. 179XX.- Chantaje sexual/Sextorsión e) Art. 179...- Exposición a contenidos nocivos

					<p>f) Art. 179...- Explotación sexual en línea</p> <p>g) Art. 179...- Materiales de abuso sexual generados de forma digital.</p> <p>h) Art. 179...- <i>Quitting</i></p> <p>i) Art. 179...- Trasmisión delictiva en vivo/<i>Streaming</i> delictivo.</p> <p>j) Art. 179...- Paliza feliz/<i>Happy slapping</i>.</p>
4	06.04.2021	Memorando Nro. AN-CCMM-2021-0026-M	As. Mercedes Cuesta	<p>Presenta sus observaciones y aportes al "PROYECTO DE LEY ORGÁNICA REFORMATORIA DEL CÓDIGO ORGÁNICO INTEGRAL PENAL Y DE LA LEY ORGÁNICA INTEGRAL PARA PREVENIR Y ERRADICAR LA VIOLENCIA CONTRA LAS MUJERES, PARA PREVENIR Y SANCIONAR LA VIOLENCIA SEXUAL DIGITAL".</p>	<p>1. Observaciones al Art. 166.1. Ciberacoso sexual.</p> <p>2. Observaciones al Art. 178.1. divulgación de contenido sexual explícito sin consentimiento.</p> <p>3. Observaciones al Art. 103.- Pornografía con utilización de niñas, niños o adolescentes.</p>

5	09.04.2021	OF-011- WAM-2021	As. Wilma Andrade	Solicitan ser recibidas en Comisión General ante la Comisión, para presentar sus argumentos en apoyo a la despenalización del aborto en caso de violación en el marco de la propuesta que hace la As. Wilma Andrade.	Presenta su propuesta de despenalización del aborto para casos de violación, dentro del presente paquete de reformas al COIP que se está analizando en esta Comisión.
6	15.04.2021	s/n	Dra. Virginia Gómez de la Torre, Directora Fundación Desafío Coalición Nacional de Mujeres en el Ecuador	Solicitan ser recibidas en Comisión General ante la Comisión, para presentar sus argumentos en apoyo a la despenalización del aborto en caso de violación en el marco de la propuesta que hace la As. Wilma Andrade.	Argumentos en apoyo a la despenalización del aborto en caso de violación en el marco de la propuesta que hace la As. Wilma Andrade.
7	20.04.2021	s/n	Ana Cristina Vera Sánchez, Directora Ejecutiva del Centro de Apoyo y Protección de los Derechos Humanos, Surkuna	Solicitan ser recibidas en Comisión General ante la Comisión, para presentar sus argumentos en apoyo a la despenalización del aborto en caso de violación en el marco de la propuesta que hace la As. Wilma Andrade.	Argumentos en apoyo a la despenalización del aborto en caso de violación en el marco de la propuesta que hace la As. Wilma Andrade.

8	23.04.2021	s/n	Dra. Virginia Gómez de la Torre, Directora Fundación Desafío Coalición Nacional de Mujeres en el Ecuador	Presentan la ponencia y cifras expuestas ante la Comisión.	Argumentos en apoyo a la despenalización del aborto en caso de violación en el marco de la propuesta que hace la As. Wilma Andrade.
---	------------	-----	--	--	---

4.1.1. Sistematización y análisis de Observaciones.

Del total de observaciones y aportes⁵ recibidos tanto en el desarrollo del Primer Debate del Pleno de la Asamblea Nacional, así como por escrito, toda vez que han sido analizados y sistematizados por el equipo técnico de la Comisión, así como conocidos y debatidos por las y los legisladores miembros de esta mesa legislativa, se han acogido un total del 92%.

Así también, del cien por ciento de observaciones recibidas, únicamente un 8% no fueron acogidas, ya sea porque no correspondían, porque fueron presentadas sin un sustento técnico jurídico de respaldo; o, en su defecto, porque contravenían a la Constitución de la República del Ecuador.

A continuación, la Tabla No. 6, detalla las observaciones y aportes:

Tabla N° 6

SISTEMATIZACIÓN DE OBSERVACIONES PRESENTADOS POR ESCRITO

No.	REMITENTE	ART.	OBSERVACIÓN / APORTE
1	Centro Ecuatoriano para la Promoción y Acción de la Mujer — CEPAM	Hostigamiento	Propone el siguiente texto alternativo: <i>“Art. 163A.- Hostigamiento. — La persona que sin contar con autorización judicial vigile, acose o hostigue de forma sistemática a través de dispositivos electrónicos y tecnológicas, insistente y reiterada, será sancionada con una pena privativa de la libertad de seis meses a un</i>

⁵ Se recibieron un total de 83 observaciones. 44 en el Primer Debate y 39 por escrito.

			<i>año, cuando concorra algunas de las siguientes circunstancias:"</i>
2	Centro Ecuatoriano para la Promoción y Acción de la Mujer — CEPAM	Sexting	Propone el siguiente texto alternativo: "179A.- Sexting. - La persona que por cualquier medio divulgue, difunda, revele, viralice o ceda a terceros contenidos, imágenes, audios o grabaciones audiovisuales que la persona afectada sin su consentimiento le hubiese confiado de su intimidad, será sancionada con una pena privativa de la libertad de uno a tres años, cuando concurren las siguientes circunstancias:"
3	Dr. Luis Benigno Gallegos Chiriboga, Ministro de Relaciones Exteriores y Movilidad Humana.	Interceptación ilegal de datos	<p>Artículo 230.- Interceptación ilegal de datos Será sancionada con pena privativa de libertad de tres a cinco años:</p> <p>1. La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma comunicaciones no públicas de datos informáticos, en su origen, destino o en el interior de un sistema informático.</p> <p>2. La persona que ilegítimamente diseñe, desarrolle, ejecute, produzca, programe, posea, venda, distribuya o, de cualquier otra forma, disemine o introduzca en uno o más sistemas informáticos, dispositivos, programas u otros datos informáticos destinados a practicar crímenes en contra de sistemas informáticos o datos, o envíe mensajes, códigos de accesos o contraseñas, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.</p>

<p style="text-align: center;">4</p>		<p style="text-align: center;">Ataque a la integridad de sistemas informáticos.</p>	<p>Artículo 232.- Ataque a la integridad de sistemas informáticos.</p> <p>La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena será sancionada la persona que:</p> <ol style="list-style-type: none"> 1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo. 2. Introduzca, transmita, dañe, borre, deteriore, altere o suprima datos informáticos, con el propósito de obstaculizar de forma grave, deliberada e ilegítima al funcionamiento de un sistema informático.
<p style="text-align: center;">5</p>		<p style="text-align: center;">Acceso no consentido a un sistema informático, telemático o de telecomunicaciones</p>	<p>Artículo 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones</p> <ol style="list-style-type: none"> 1. La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, será sancionada con la pena privativa de la libertad de XXX a XXX años. 2. Si la persona que accede al sistema lo hace para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o re direccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los

			<p>proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años.</p>
6		<p>Definiciones</p>	<p>Artículo 228-A. - Definiciones Para los efectos del presente Código Orgánico, se considera:</p> <p>a) «Datos informáticos», toda representación de hechos, informaciones o conceptos de una forma adecuada para su procesamiento en un sistema informático, incluidos los programas capaces de hacer que un sistema informático ejecute una función;</p> <p>b) «Datos de tráfico», los datos informáticos relativos a una comunicación efectuada por medio de un sistema informático, generados por este sistema como elemento de una cadena de comunicación, indicando el origen de la comunicación, su destino, su trayecto, la hora, la fecha, el tamaño, duración o el tipo de servicio subyacente.</p> <p>c) «Proveedor de servicios»; cualquier entidad, pública o privada, que proporciona a los usuarios de sus servicios la capacidad de comunicarse a través de un sistema informático, así como cualquier otra entidad que procesa o almacena datos informáticos en nombre y por cuenta de aquella entidad proveedora o de sus usuarios, y</p> <p>d) «Sistema informático», cualquier dispositivo o conjunto de dispositivos interconectados o asociados, en que uno o varios de ellos desarrolla, ejecutando un programa, el tratamiento automatizado de datos informáticos.</p>

7		<p>Falsificación informática</p>	<p>Artículo 234-A. - Falsificación informática</p> <p>1. La persona que, con intención de provocar un engaño en las relaciones jurídicas, introducir, modificar, eliminar o suprimir datos informáticos, o interferir de cualquier otra forma en el tratamiento informático de datos, produciendo datos o documentos no genuinos, será sancionada con pena privativa de libertad de tres a cinco años.</p> <p>2. Quien, actuando con intención de causar un perjuicio a otro o de obtener un beneficio ilegítimo para sí o para un tercero, use un documento producido a partir de datos informáticos que fueran objeto de los actos referidos en el número 1, será sancionado con la misma pena.</p>
8		<p>Agravación de las penas</p>	<p>Artículo 234-B. - Agravación de las penas</p> <p>La práctica de los hechos que se describen en los Artículos 232 y 234 será sancionada con pena agravada en un tercio de su pena máxima si lograr perturbar de forma grave o duradera a un sistema informático que apoye una actividad destinada a asegurar funciones sociales críticas, como cadenas de abastecimiento, salud, seguridad y bienestar económico de las personas, o funcionamiento regular de los Servicios públicos.</p>
9		<p>Responsabilidad de personas jurídicas.</p>	<p>Artículo 234-C. - Responsabilidad de personas jurídicas.</p> <p>A los delitos de esta Sección es aplicable la responsabilidad prevista en el Artículo 49 y 71 de este código.</p>
10		<p>Interceptación de las comunicaciones en cooperación internacional.</p>	<p>Artículo 477-A. - Interceptación de las comunicaciones en cooperación internacional.</p> <p>En ejecución de una petición de una autoridad extranjera competente, puede ser ordenada la interceptación de transmisiones de datos informáticos realizadas por medio de un sistema informático ubicado en el Ecuador, si así se prevé en acuerdo, tratado o convenio internacional y si se trata de situación en la que dicha interceptación está</p>

			<p>permitida en un caso nacional de características similares, respetándose el procedimiento y observándose los límites y garantías previstos en el derecho interno.</p>
11		<p>Aseguramiento de datos</p>	<p>SECCIÓN CUARTA. Pruebas Digitales.</p> <p>Artículo 495-A. - Aseguramiento de datos.</p> <p>1. El fiscal a cargo de la investigación podrá ordenar a una o varias personas naturales o jurídicas que aseguren o conserven datos informáticos concretos, almacenados en un sistema informático o en un dispositivo de almacenamiento informático, que estén bajo su disposición control, cuando tenga motivos para sospechar que los datos pueden ser alterados o suprimidos. La orden deberá especificar los datos concretos que se pretende conservar y la medida ordenada no podrá exceder de noventa días, prorrogables por igual periodo si se mantienen los motivos que fundamentaron la orden.</p> <p>2. La persona requerida deberá procurar los medios necesarios para preservar de inmediato los datos en cuestión y queda obligado a mantener secreto de la orden recibida durante el tiempo que dure la medida, bajo el apercibimiento de incurrir en responsabilidad penal.</p> <p>3. El proveedor de servicios de una comunicación que haya recibido la orden de aseguramiento de datos relativos al tráfico de una comunicación informará de inmediato a la autoridad que emitió la orden cuando advierta que la comunicación bajo investigación ha sido efectuada con la participación de otros proveedores de servicios a fin de que se puedan arbitrar las medidas necesarias para solicitar a dichos proveedores el aseguramiento de los datos.</p>

<p>12</p>	<p>Orden de presentación</p>	<p>Artículo 495-B. - Orden de presentación.</p> <p>1. El fiscal, o el juez cuando la naturaleza de los datos así lo requiera, podrá ordenar a cualquier persona natural o jurídica, que presente, remita o entregue datos alojados en un sistema informático que este bajo su poder o control y que se vinculen con la investigación de un delito concreto.</p> <p>2. Asimismo, el fiscal podrá ordenar a toda persona natural o jurídica que preste un servicio de comunicaciones o a proveedores de servicios que presten sus servicios en el territorio de Ecuador, la entrega de datos de los usuarios o abonados o los datos de identificación y facturación con los que cuente.</p> <p>3. Las ordenes podrán contener la indicación de que la medida deberá mantenerse en secreto bajo el apercibimiento de responsabilidad penal.</p>
<p>13</p>	<p>Búsqueda e incautación de datos informáticos.</p>	<p>Artículo 495-C. - Búsqueda e incautación de datos informáticos.</p> <p>1. El juez podrá ordenar a requerimiento de parte, el registro de un sistema informático o de una parte de éste, o de un medio de almacenamiento de datos informáticos o electrónicos, con el objeto de:</p> <p>A. Incautar los componentes físicos del sistema y, si fuera necesario, los dispositivos para su lectura,</p> <p>B. Obtener copia de los datos en un soporte autónomo o,</p> <p>C. Preservar por medios tecnológicos los datos de interés para la investigación. Regirán en cuanto sean aplicables las normas generales y las mismas limitaciones dispuestas para el secuestro de documentos y correspondencia epistolar.</p> <p>2. En los supuestos en los que durante la</p>

			<p>ejecución de una medida de registro e incautación de datos de un sistema informático previstos en el párrafo anterior surjan elementos que permitan considerar que los datos buscados se encuentran almacenados en otro dispositivo o sistema Informático al que se tiene acceso lícito desde el dispositivo o sistema inicial, quienes llevan adelante la medida podrán extenderla o ampliar el registro al otro sistema. La ampliación del registro a los fines de la incautación de datos deberá ser autorizada por el juez salvo que estuviera prevista en la orden original.</p>
14		<p>Cooperación internacional</p>	<p>SECCIÓN QUINTA Obtención de Prueba por Medio de Cooperación Internacional</p> <p>Artículo 495-D. - Cooperación internacional Las autoridades nacionales competentes cooperarán con las autoridades extranjeras competentes en las investigaciones o procedimientos relativos a delitos relacionados con los sistemas informáticos o los datos, así como para la obtención de pruebas de un delito, en formato digital.</p>

<p>15</p>		<p>Preservación y divulgación expedita de datos informáticos en la cooperación internacional.</p>	<p>Artículo 497-A. - Preservación y divulgación expedita de datos informáticos en la cooperación internacional.</p> <p>1 - Se puede solicitar al Ecuador la preservación expedita de datos informáticos almacenados en un sistema informático aquí ubicado, con el objetivo de presentar una solicitud de asistencia para la búsqueda, incautación y divulgación de los mismos.</p> <p>2 - La solicitud especificará:</p> <p>A. La autoridad que solicita la preservación;</p> <p>B. El delito que está siendo investigado, así como un breve Resumen de los hechos conexos;</p> <p>C. Los datos informáticos que deben conservarse y su relación con el delito;</p> <p>D. Toda la información disponible para identificar a la persona responsable de los datos informáticos o la ubicación del sistema informático;</p> <p>E. La necesidad de la preservación, y</p> <p>F. La intención de presentar una solicitud de ayuda para la búsqueda, incautación y difusión de datos.</p> <p>3 - En la ejecución de una solicitud de autoridad extranjera competente en virtud de los números anteriores, el fiscal (la autoridad competente) dará la orden a quién tenga el control o disponibilidad de estos datos, incluido el proveedor de servicios, para que este los preserve.</p> <p>4 - La orden de preservación especificara, bajo pena de nulidad:</p> <p>A. La naturaleza de los datos;</p>
-----------	--	--	--

			<p>B. Si se conocen, su origen y su destino, y</p> <p>C. El período de tiempo durante el cual los datos deben conservarse hasta un máximo de tres meses.</p> <p>5. - En cumplimiento de la orden de preservación dirigida hacia él, quien tenga el control o la disponibilidad de estos datos, incluyendo el proveedor de servicios, preservará de inmediato los datos en cuestión por el periodo especificado, protegiendo y conservando su integridad.</p> <p>6. - El fiscal (la autoridad competente) podrá ordenar la renovación de la medida por periodos sujetos al límite previsto en c) del número 5, siempre que se verifiquen sus requisitos de admisibilidad, hasta un máximo un año.</p> <p>7. - Cuando sea presentada la solicitud dada en el número 1, el fiscal (la autoridad competente) determinará la preservación de los datos hasta la adopción de una decisión definitiva sobre la solicitud</p> <p>8. - Los datos preservados en virtud del presente artículo se concederán únicamente:</p> <p>A. Al fiscal (la autoridad competente), en la ejecución de la solicitud de ayuda contemplada en el número 1, de la misma manera que podría hacerse en un caso nacional de características similares;</p> <p>B. A la autoridad nacional que emitió la orden de preservación, en las mismas condiciones que podrían realizarse en un caso similar nacional.</p> <p>9.- Las disposiciones de los apartados 1 y 2, se aplicarán, con las debidas adaptaciones, a las peticiones formuladas por las autoridades del Ecuador a autoridades extranjeras.</p>
--	--	--	--

16		<p>Motivos de denegación</p>	<p>Artículo 497-B. - Motivos de denegación.</p> <p>1. - La solicitud de preservación o divulgación expedita de datos informáticos será denegada cuando:</p> <p>A. Los datos informáticos en cuestión se refieren a un delito político o delito conexo de acuerdo con los conceptos del derecho del Ecuador; y</p> <p>B. Atenten contra la soberanía, seguridad, orden público u otros intereses del Ecuador.</p> <p>2 - La solicitud de preservación expedita de datos informáticos podrá aún ser denegada si existieren motivos razonables para creer que la ejecución de la subsecuente solicitud de ayuda para fines de búsqueda, incautación y divulgación de tales datos será rechazada por falta de comprobación del requisito de la doble incriminación.</p>
17		<p>Acceso a datos informáticos en la cooperación internacional</p>	<p>Artículo 497-C. - Acceso a datos informáticos en la cooperación internacional</p> <p>1. - En ejecución de una solicitud de autoridad extranjera competente, y de acuerdo con las normas de derecho nacional, se procederá al registro e incautación y la divulgación de datos almacenados en un sistema informático ubicado en el Ecuador, cuando se trate de una situación en que el registro e incautación son admisibles en un caso nacional de características similares.</p> <p>2. - Las autoridades nacionales actuarán, en el ámbito de sus competencias, tan pronto como sea posible, cuando existieran razones para creer que los datos informáticos en cuestión son especialmente vulnerables a su pérdida o modificación, o cuando la cooperación rápida esté prevista en un instrumento internacional aplicable.</p> <p>3. - Las disposiciones del número 1 se aplicarán, con las debidas adaptaciones, a las peticiones formuladas por las autoridades del Ecuador a autoridades extranjeras.</p>

18		<p>Acceso transfronterizo a datos informáticos almacenados de acceso público o con consentimiento.</p>	<p>Artículo 497-D Acceso transfronterizo a datos informáticos almacenados de acceso público o con consentimiento.</p> <p>1. Las autoridades extranjeras competentes, podrán:</p> <p>A. Acceder a datos informáticos almacenados en un sistema informático ubicado en el Ecuador, cuando éstos estén a disposición del público;</p> <p>B. Recibir o acceder, por medio de un sistema informático ubicado en su territorio, a datos informáticos almacenados en el Ecuador, con el consentimiento legal y voluntario de la persona legalmente autorizada a revelarlos.</p> <p>2. Las mismas facultades tendrán las autoridades del Ecuador, con relación con datos informáticos alojados en el extranjero.</p>
19		<p>Punto permanente de contacto para la cooperación internacional</p>	<p>Artículo 497-E. - Punto permanente de contacto para la cooperación internacional</p> <p>1. - A los fines de la cooperación internacional, la Fiscalía General del Estado mantendrá una estructura que garantice un punto de contacto disponible en todo momento, las veinticuatro horas del día, los siete días de la semana.</p> <p>2. - Esta estructura podrá ser contactada por sus pares extranjeros, con arreglo a los acuerdos, tratados o convenios a los cuales el Ecuador está obligado, o en ejecución de protocolos de cooperación internacional con organismos judiciales o policiales.</p> <p>3. - La asistencia inmediata que ofrece este punto de contacto permanente incluye:</p> <p>A. La prestación de asesoramiento técnico a otros puntos de contacto;</p> <p>B. La preservación expedita de datos en casos de urgencia o peligro en el retraso, en</p>

			<p>conformidad con el artículo siguiente;</p> <p>C. La recopilación de pruebas para las que tiene jurisdicción en casos de urgencia o de peligro en el retraso;</p> <p>D. La localización de sospechosos y el suministro de información de carácter jurídico en casos de urgencia o de peligro en el retraso.</p>
20	<p>Dr. Francisco Ramiro Cevallos Tejada, Secretario Técnico Consejo Nacional para la Igualdad Intergeneracional</p>	<p>Hostigamiento</p>	<p>El marco normativo ecuatoriano, no prevé autorización judicial alguna para vigilar, acosar u hostigar. Se recomienda revisar la redacción de la propuesta de artículo, inciso primero.</p> <p>Se recomienda incluir en el acápite tres, el robo o suplantación de identidad en el entorno digital.</p> <p>Asimismo, considerando la doctrina de protección integral de niñas, niños y adolescentes, se recomienda endurecer la pena cuando las víctimas de este delito sean niñas, niños y adolescentes.</p>

21		<p>Violencia Sexual Digital</p>	<p>Según información de UNICEF, dos terceras partes de adolescentes de América Latina y el Caribe, y de África Subsahariana, creen que los jóvenes corren el peligro de ser abusados sexualmente o aprovechados en línea; siendo esta creencia mayor que en el resto de regiones del mundo (UNICEF, 2016). El trabajo desarrollado por la Secretaría General de la OEA y el Instituto Interamericano del Niño, la Niña y Adolescentes (IIN), da cuenta que las niñas, los niños y adolescentes están al tanto de ciertos delitos, en particular del <i>ciberbullying</i> en mayor medida y del <i>sexting</i>; aunque otras conductas no son tan conocidas aún. De acuerdo a un estudio de Unicef del año 2015 se identificó que, en el Ecuador, el 60% de niñas, niños y adolescentes ha sufrido, alguna vez, de acoso escolar. En muchos de estos casos, se han usado medios digitales para la realización de estas conductas inadecuadas que incluso han degenerado en suicidio (CNII, 2020).</p> <p>Con base a esta información, en relación a la violencia sexual digital, se recomienda considerar que este tipo de delito no solo puede causar “<i>daño o perjuicio, afectación en su psiquis o discrimine y que atenten contra la imagen y la dignidad de cualquier persona</i>”, sino que producto de la afectación a la salud emocional de la víctima, podría derivar en conductas auto lesivas como cortarse o suicidarse; incentivar al uso de alcohol, drogas y tabaco, abuso emocional, contacto con grupos que promueven el odio y la intolerancia; trastornos del comportamiento o de la alimentación, entre otros.</p> <p>Frente a ello, recordar que la Convención sobre los Derechos del Niño, establece que las niñas, niños y adolescentes, se encuentran en un proceso de madurez física y mental y por tanto necesitan protección y cuidados especiales, incluso la debida protección legal, tanto antes como después del nacimiento; adicionalmente, reconoce</p>
----	--	--	---

que en todos los países del mundo hay niños que viven en condiciones excepcionalmente difíciles y que requieren especial consideración (Preámbulo). En ese sentido, todas las medidas relacionadas con estos grupos de atención, que tomen las autoridades, una consideración primordial a la que se atenderá será el principio del interés superior del niño (artículo 3 de la Convención sobre los Derechos del Niño); el mismo que, para aplicarlo, en el proceso de toma de decisiones, precisa valorar también la posibilidad de prevenir riesgos y daños futuros, y otras consecuencias (Comité de los Derechos del Niño, Observación General 14, párrafo 74).

Se recomienda incluir una excepcionalidad o aclaración respecto a que, en el caso de niñez y adolescencia, no existe la figura de consentimiento porque hay una relación de poder, coacción, sometimiento sobre las niñas, niños y adolescentes. Además, al estar en un proceso de crecimiento y desarrollo, se parte del supuesto de que no necesariamente el niño, niña o adolescente comprende las implicaciones y consecuencias de una determinada acción y sus consecuencias. Considerar también, los términos *“hipersexualización infantil”*, que han sido definidos como: *“la sexualización de las expresiones, posturas o códigos de la vestimenta considerados como demasiado precoces”* (Bailey, 2001). Ello con el fin de tomar en cuenta como agravante, el que el padre, madre o cualquier familiar o persona hipersexualice a una niña, niño o adolescente, con fines sexuales.

22		<p>Ciberacoso sexual.</p>	<p>En relación al ciberacoso sexual, que según se menciona se lo realiza “<i>con el objeto de intimidar, dominar, presionar o amenazar a la víctima, con el objeto de perjudicar o menoscabar su imagen, dignidad, privacidad e intimidad sexuales</i>”, al igual que la violencia sexual digital, se recomienda también considerar que ello puede repercutir en la salud emocional de la víctima y posteriormente provocar conductas auto lesivas como cortarse o suicidarse; incentivar al uso de alcohol, drogas y tabaco, abuso emocional, contacto con grupos que promueven el odio y la intolerancia; trastornos del comportamiento o de la alimentación, entre otros.. Respeto de lo cual, recalamos lo manifestado por la Convención sobre los Derechos del Niño y las Observaciones Generales del Comité de los Derechos del Niño, en particular la Observación General 14, antes expuesto.</p> <p>Por otro lado, es importante se considere que las tecnologías de la información avanzan y se actualizan en el tiempo; por lo que, para que la norma no sea restrictiva, se debería plantear en el inciso segundo que se entiende por tecnologías de la información y la comunicación, al conjunto de recursos tecnológicos presentes o futuros, con eso evitamos restricción en la norma.</p> <p>Si bien en el siguiente artículo se amplía el tema, es importante se considere que la violencia sexual digital dentro del entorno familiar no únicamente se supedita a la pareja o ex pareja. El inciso tercero es restrictivo y no observa la realidad.</p>
----	--	----------------------------------	---

23		<p>Disposiciones comunes a los delitos de violencia sexual digital</p>	<p>En relación a la propuesta de “Art. 175.3.- Disposiciones comunes a los delitos de violencia sexual digital, en lo referente a que el Juez Penal” como medida cautelar suspenderá la patria potestad, tutoría, curatela y cualquier otra modalidad de cuidado sobre la víctima a fin de proteger sus derechos”, se recomienda considerar, el que el Juez Penal una vez que haya emitido estas medidas cautelares, también pueda solicitar medidas de protección a las Juntas Cantonales y Metropolitanas de Protección de Derechos o Jueces de la Familia Mujer Niñez y Adolescencia, para un mejor abordaje, desde la integralidad de los derechos de niñas, niños y adolescentes, es decir, para que, adicional al derecho a la salud física y emocional, se puedan garantizar otros derechos como la salud y educación. Recordar que las JCPD tienen como función disponer las medidas administrativas de protección que sean necesarias para proteger el derecho amenazado de niñas, niños y adolescentes o restituir el derecho violado, para lo cual, articularán sus acciones con los órganos judiciales y funcionarios públicos de la administración central y seccional, de conformidad con el artículo 206 literales a), c), d) y f).</p>
----	--	---	--

24		<p>Sexting</p>	<p>Se recomienda tomar en cuenta que niñas, niños y adolescentes por estar en proceso de madurez física y mental, no dan consentimiento; por lo tanto, necesitan protección y cuidados especiales (Preámbulo de la Convención sobre los Derechos del Niño).</p> <p>Adicionalmente, hoy en día con los avances tecnológicos y el aumento del movimiento entre países, la idea de tecnologías y la utilización del Internet han aumentado, virtualizando las relaciones interpersonales. Uno de los más notorios avances tecnológicos es el de Internet, que permite al usuario encontrar información sobre cualquier cosa y en cualquier lugar del mundo, como, la pornografía infantil, entre otras situaciones, como el ciberacoso, <i>grooming</i>, <i>sexting</i>, robo de identidad y otros delitos (IIN, 2011).</p> <p>Según Unicef (2015), un tercio de adolescentes usa Internet durante dos o tres horas al día, un 14% lo utiliza más de ocho horas diarias; mientras que, según cifras de la Organización de las Naciones Unidas - ONU y la Fundación Telefónica, el 55 % de los jóvenes latinoamericanos ha sido víctimas de Ciberacoso (CNII, 2020). De ahí la importancia de desarrollar otros tipos de delitos que no están siendo considerados dentro de esta propuesta. Se recomienda también considerar que, las niñas, niños y adolescentes no entienden las fronteras sociales y pueden publicar información personal en línea, por ejemplo, en sus perfiles de redes sociales, que no debería hacerse pública. Esto puede ser cualquier tipo de imágenes de momentos personales incómodos o sus direcciones caseras. También que puede considerarse una forma de acoso sexual el que la niña, niño y adolescente puede ser presionado a enviar una foto a su novio/a o compañero, quien después la distribuye sin su consentimiento (ECPAT, 2016, recogido por CNII, 2020).</p>
----	--	-----------------------	---

<p>25</p>		<p>Violencia contra niñas, niños y adolescentes a través de tecnologías de la información y las comunicaciones</p>	<p>Art. 179XX.- Violencia contra niñas, niños y adolescentes a través de tecnologías de la información y las comunicaciones. - Es cualquier manifestación de violencia expresada o ejercida a través cualquier medio de telecomunicación o tecnologías de la información y comunicación, incluyendo las redes sociales, plataformas virtuales o cualquier otro; que permiten el acceso no autorizado o secreto a las niñas, niños y adolescentes como potenciales víctimas de violencia física, sexual o psicológica, como medios de reclutamiento para actividades ilegales o ilícitas y también como emisores de información agresiva en contra de otras niñas, niños y adolescentes como mecanismo para ejercer violencia entre pares. Las TIC presentan riesgos para las niñas, niños y adolescentes en las siguientes esferas:</p> <p>a. Los abusos sexuales cometidos contra niñas, niños y adolescentes para producir imágenes y grabaciones de abusos a niñas, niños y adolescentes a través de Internet y otras TIC;</p> <p>b. El hecho de tomar, retocar, permitir que se tomen, distribuir, mostrar, poseer o publicitar fotografías o pseudo fotografías (<i>morphing</i>) y vídeos que expongan la imagen y la intimidad de las niñas, niños y adolescentes; y,</p> <p>c. La utilización de las TIC por las niñas, niños y adolescentes:</p> <p>i. En condición de receptores de información, las niñas, niños y adolescentes pueden estar expuestos a publicidad, correo electrónico no deseado, patrocinios, información personal y contenidos agresivos, violentos, de incitación al odio, tendenciosos, racistas, discriminatorios, pornográficos, desagradables y/o engañosos que son o pueden ser perjudiciales; Revisar redacción, incorporar observaciones de la supervisión de adultos.</p>
------------------	--	---	---

			<p>ii. Las niñas, niños y adolescentes que mantienen contactos con otras niñas, niños y adolescentes a través de TIC pueden ser objeto de intimidación, hostigamiento o acoso (utilización de métodos para atraer a las niñas, niños y adolescentes con fines sexuales) o coacción, ser engañados o persuadidos a citarse personalmente con extraños o ser "<i>captados</i>" para hacerlos participar en actividades sexuales y obtener de ellos información personal; y,</p> <p>iii. En condición de agentes, las niñas, niños y adolescentes pueden intimidar u hostigar a otros, participar en juegos que afecten negativamente a su desarrollo integral, crear y publicar material sexual inapropiado, dar información o consejos equivocados o realizar descargas y ataques piratas y participar en juegos de azar, estafas financieras o actividades terroristas.</p>
26		Grooming	<p>Art. 179XX.- <i>Grooming</i>: Estrategias que realiza un adulto para ganarse la confianza de un niño, niña y adolescente, a través de Internet, con el propósito de abusarlo o explotarlo sexualmente. Es importante expresar que siempre es un adulto quien ejerce el <i>grooming</i>.</p> <p>Existen dos tipos de <i>grooming</i>:</p> <ol style="list-style-type: none"> 1. Cuando no existe la fase previa de relación y generación de confianza, el acosador logra obtener fotos o videos sexuales de las niñas, niños y/o adolescentes, con la intención de extorsionarlos con difundir dicho material, a cambio de acceder a encuentro personal. 2. Cuando existe una fase previa donde el acosador busca generar confianza en la niña, niño o adolescente, logrando que los mismos entreguen material sexual para volverlo objeto de chantaje, valiéndose de distintas herramientas, como hacerse pasar por un chico o chica menor, manipular a través de los gustos y preferencias de la

		víctima, utilizar el tiempo para fortalecer el vínculo.
27	Flaming	Art. 179XX.- <i>Flaming</i> . - Mensajes a través redes sociales o comunidades virtuales con lenguaje violento, agresivo y/o vulgar, el cual es reiterativo en su intención de humillar e intimidar a una persona.
28	Chantaje sexual/Sextorsión	Art. 179XX.- Chantaje sexual / Sextorsión. - Es el chantaje a una persona, amenazándola con difundir imágenes o videos sexuales autogenerados por estos, con la intención de mantener relaciones sexuales y/o continuar con la explotación sexual.
29	Exposición a contenidos nocivos	Art. 179...- Exposición a contenidos nocivos: Se refiere al acceso o exposición de niñas, niños y adolescentes, de forma intencionada a contenido violento sexualizado, o generador de odio, siendo perjudicial para su desarrollo.
30	Explotación sexual en línea	Art. 179...-Explotación sexual en línea. - Incluye todos los actos de naturaleza sexual cometidos contra una persona a través de la utilización de Internet, como medio para explotarlos sexualmente. Así mismo, incluye el uso de las TIC como medio para producir o provocar la explotación sexual de la persona, que da como resultado imágenes o materiales que documentan la explotación sexual con la intención de producir, difundir, comprar y vender.
31	Outing	Art. 179...- <i>Outing</i> .- Es la publicación o difusión de imágenes, mensajes, correos íntimos u otros datos íntimos sobre la sexualidad de una persona, sin su consentimiento, que afecte a su imagen, dignidad, honor, reputación e integridad psicológica, en virtud de que ha querido mantener esta información en secreto.
32	Trasmisión en vivo/Streaming	Art. 179...- Trasmisión en vivo/ <i>Streaming</i> . - Es la transmisión en vivo relacionada con una conducta nociva y criminal, en la que se muestra prácticas de abuso sexual contra una persona, a través de prostitución, espectáculos pornográficos o elaboración de material de carácter pornográfico que son transmitidas en vivo.

33		<p>Paliza feliz/Happy slapping</p>	<p>Art. 179...- Paliza feliz / <i>Happy slapping</i>. - Es la acción de una persona o grupo, que golpea a otra persona, mientras se graba el incidente con la cámara de un teléfono celular, tablet, u otro dispositivo digital de video, con el fin de burlarse o ridiculizar a la víctima o víctimas. En este tipo de agresiones, pueden estar inmersas agresiones de índole sexual.</p>
34		<p>Disposición General</p>	<p>En relación a las definiciones antes expuestas, se solicita considerar como disposiciones comunes y agravantes cuando la víctima sea menor de dieciocho años de edad o con discapacidad, o por cualquier causa no pueda resistirlo, para definir la pena. Adicionalmente, el que dichas acciones provoquen en la víctima suicidio o intento de suicidio.</p> <p>Esto bajo las consideraciones anteriormente expuestas, el que a raíz de la emergencia sanitaria suscitada en el mundo, varios organismos internacionales de derechos humanos se han pronunciado y emitido recomendaciones a los países, entre ellos, el Comité de los Derechos del Niño de las Naciones Unidas, el mismo que <i>“expresa su preocupación por la situación de los niños en todo el mundo, particularmente en situaciones de vulnerabilidad, debido a los efectos de la pandemia de COVID-19”</i>; y, la Organización de Estados Americanos (OEA), que ha señalado que esta pandemia nos afecta directa e indirectamente a todos, no obstante, tendría un mayor impacto para las personas en situación de vulnerabilidad, como son los pueblos indígenas, afrodescendientes, personas adultas mayores, personas con discapacidad, migrantes, refugiados y personas LGBTI, niñas, niños y adolescentes y mujeres, considerando que en situaciones de emergencia, el acceso y goce de derechos básicos podría verse limitado (OEA, 2020).</p>

35		Artículo 10. LOPEVCM	Se recomienda considerar los mismos argumentos y propuestas de artículo establecidos por el CNII en relación a las Reformas al Código Integral Penal, propuesta de artículos: Art. 175.1.- Violencia sexual digital; Art. 175.2.- El ciberacoso sexual; y. Art. 179A.- <i>Sexting</i> .
36	As. Mercedes Cuesta	Ciberacoso sexual	<p>El artículo 1 del informe propone incluir luego del artículo 166 del Código Orgánico Integral Penal, un artículo que tipifique el ciberacoso sexual. Así, en el texto consta una referencia a la utilización de medios tecnológicos o digitales presentes o futuros. Esto último constituye una referencia antitécnica pues el catálogo penal debe poseer la suficiente solidez para proyectarse y ser aplicable en tiempo presente. Se sugiere eliminar la referencia “o futuros”.</p> <p>Por otro lado, el mismo artículo incluye dentro de las sanciones, para quien sea sentenciado por el delito de ciberacoso sexual, la inhabilitación para el acceso a medios digitales. Se comprende la intención de los comisionados para proteger a las víctimas, no obstante esta sanción es de difícil aplicabilidad por la diversidad de medios digitales y la universalidad de las tecnologías de la información; por lo que se vuelve ineficaz. Debido a lo expuesto, se sugiere eliminar el inciso quinto del artículo 166.1.</p>
37		Divulgación de contenido sexual explícito sin consentimiento	<p>El artículo 3 del informe propone que luego del artículo 178 del Código Orgánico Integral Penal, se agregue una disposición 178.1 sobre la divulgación de contenido sexual explícito sin consentimiento.</p> <p>El primer párrafo describe la divulgación, revelación o tratamiento indebido de datos personales, mensajes, imágenes, audios o grabaciones audiovisuales con contenido sexual explícito, cuando la persona afectada le hubiese confiado de su intimidad. Sin perjuicio de lo indicado, este despacho</p>

sugiere considerar la redacción que consta en la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal español[1] que hace referencia a la difusión, revelación a terceros de imágenes o grabaciones audiovisuales que hubiera obtenido con consentimiento en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros.

De su parte, el artículo ha incluido que para el tipo penal de la Divulgación de contenido sexual explícito sin consentimiento, deberán concurrir: *“2. Que la divulgación, difusión, revelación, viralización o tratamiento indebido cause o haya causado daño o perjuicio, afectación en su psiquis o discrimine o atente al derecho a la protección de datos personales y autodeterminación informativa, a la honra y buen nombre, a la imagen; o, a la intimidad personal de la víctima”*. Esta condición complica la acción penal y acarrearía trámites pre procesales para la víctima. Se sugiere considerar eliminar este requisito en el tipo penal.

Por otro lado, y con el objeto de aportar mayor claridad a la redacción, este despacho sugiere reemplazar el octavo párrafo por el siguiente: *“Cuando este ilícito sea cometido por miembros del núcleo familiar, cónyuge, o por persona que esté o haya estado unida a él por relación de afectividad, aun sin convivencia, se aplicará el máximo de pena establecida en este artículo”*.

38		<p>Pornografía con utilización de niñas, niños o adolescentes</p>	<p>En el marco de este proyecto de Ley, este despacho considera pertinente incluir en el proyecto un artículo que reforme el artículo 103 del COIP, sobre la pornografía con utilización de niñas, niños o adolescentes; concretamente para que se incluya en el tipo penal cuando el material tuviere origen en el extranjero. Con ese antecedente, se sugiere sustituir el primer párrafo del artículo 103 por el siguiente:</p> <p><i>“Art. 103.- Pornografía con utilización de niñas, niños o adolescentes.- La persona que fotografíe, filme, grave, produzca, transmita o edite materiales visuales, audiovisuales, informáticos, electrónicos o de cualquier otro soporte físico o formato que contenga la representación visual de desnudos o semidesnudos reales o simulados de niñas, niños o adolescentes en actitud sexual, aunque el material tuviere su origen en el extranjero o fuere desconocido, será sancionada con pena privativa de libertad de trece a dieciséis años.”</i></p>
39	As. Wilma Andrade	<p>150. Aborto no punible</p>	<p>En tal sentido, planteo a usted y a todos los miembros de la comisión de Justicia y Estructura del Estado, que asuman el reto y den una respuesta a una problemática social que destroza el tejido social en el país.</p> <p>Solicito se incorpore el siguiente texto en el Proyecto de Ley Orgánica Reformatoria del Código Orgánico Integral Penal y de la Ley Orgánica Integral para Prevenir y Erradicar la Violencia Contra las Mujeres, para Prevenir y Sancionar la Violencia Sexual Digital.</p> <p>ARTÍCULO (..).- En el Código Orgánico Integral Penal, sustitúyase el segundo número del artículo 150 por el siguiente texto:</p> <p><i>“2. Si el embarazo es consecuencia de una violación.”</i></p>

4.2. Temas incluidos para Segundo Debate.

El presente informe comprende la síntesis del análisis técnico, jurídico, sistemático e integral de cada uno de los componentes teóricos y jurídicos que integran el presente proyecto de Ley, realizado a través de la sistematización y procesamiento de comparecencias, observaciones, aportes y demás insumos recibidos por diversos actores, que fueron conocidos y debatidos por las y los legisladores a lo largo de las múltiples sesiones y reuniones técnicas efectuadas, mismas que constituyeron categorías de análisis que nutrieron y retroalimentaron no solo el debate, análisis y discusión en el seno de esta Comisión, sino principalmente, el presente “PROYECTO DE LEY ORGÁNICA REFORMATIVA DEL CÓDIGO ORGÁNICO INTEGRAL PENAL PARA PREVENIR Y COMBATIR LA VIOLENCIA SEXUAL DIGITAL Y FORTALECER LA LUCHA CONTRA LOS DELITOS INFORMÁTICOS”.

5. TECNOLOGÍA E INTERNET

En la actualidad, la manera de vivir en la sociedad, ha evolucionado a pasos agigantados, ya que al desarrollarse tecnologías nuevas o avances tecnológicos, se han generado aportaciones importantes a todos los medios de comunicación y a la manera de comunicarnos. De un día para otro la vida de las personas dio un cambio inesperado al surgir la computadora y lo digital, fue un avance enorme para la sociedad. Posteriormente al surgir el internet, lo digital creó infinidad de información, a la cual podían acceder personas de todas partes del mundo, por tanto el comunicarse se volvió más rápido y fácil, sin importar el lugar en donde se quiera iniciar una comunicación, cabe mencionar que todo esto generaba un precio exageradamente bajo en comparación a lo que ahora se puede lograr con el uso del internet.

Posterior al surgimiento del internet, expertos en la materia fueron desarrollando infinidad de aplicaciones útiles para las labores y actividades que realizamos a

diario y que con el tiempo se han convertido en necesarias. Al momento de crearse los buscadores web, se nos dio libre acceso a cualquier información, ya que previamente toda esta información fue digitalizada y sigue siéndolo con el fin de compartimos el conocimiento, para hacer negocios, para crear un proceso de marketing, llevarnos al entretenimiento y el ocio. Está claro que desde el momento que abrimos una página web, estamos introduciéndonos en la cultura digital, donde nuestros valores y costumbres pasan a formar parte de distintas ideologías y perspectivas, al instante de tener que compartir la información.

Cuando escuchamos decir que *“se sustituyó lo físico por lo digital”*, cabe mencionar que anteriormente se utilizaban reglas de cálculo y máquinas de escribir, que ahora han sido remplazadas por recientes innovaciones tecnológicas que vienen brindando a la humanidad la capacidad de mejora en sus habilidades con el uso de herramientas novedosas.

“Los nuevos medios aparecen gradualmente por la metamorfosis de los medios antiguos. Cuando emergen nuevas formas de medios de comunicación, las formas antiguas generalmente no mueren, sino que continúan evolucionando y adaptándose” (Fidler, 1998).

Con el avance tecnológico de las computadoras, las formas de transmitir información se rediseñaron. Al término de la segunda guerra mundial, nuevas investigaciones en el campo de la tecnología se generaron, y las formas de poder almacenar información en equipos digitales ya no era suficiente, surgió entonces la necesidad de enviar información a miles de partes del mundo y en cortos lapsos de tiempo incluso segundos, sin tener que estar presentes o ir hasta el lugar, utilizando únicamente herramientas conectadas a una red, una red de la nueva era digital, la red de internet.

La Internet nació en EE.UU. como un proyecto de la DARPA (*Defense Advanced Research Projects Agency*). La misma buscaba intercambiar información entre los investigadores, científicos y militares, ubicados en distintos sitios distantes.

Las tecnologías pueden ayudar a que nuestro mundo sea más justo, más pacífico y más equitativo. Los avances digitales pueden apoyar y acelerar el logro de cada uno de los 17 Objetivos de Desarrollo Sostenible, desde el fin de la pobreza extrema hasta la reducción de la mortalidad materna e infantil, la promoción de la agricultura sostenible y el trabajo decente, y el logro de la alfabetización universal. Sin embargo, las tecnologías también pueden amenazar la privacidad, comprometer la seguridad y alimentar la desigualdad. Tienen implicaciones para los derechos humanos y la actividad humana. Al igual que generaciones anteriores, nosotros, gobiernos, empresas e individuos, tenemos que decidir cómo aprovechar y gestionar las nuevas tecnologías.

Hoy en día, las tecnologías digitales, como el agrupamiento de datos y la inteligencia artificial, se utilizan para rastrear y diagnosticar problemas en la agricultura, la salud y el medio ambiente, o para realizar tareas cotidianas como el desplazamiento en automóvil o el pago de una factura. Pueden usarse para defender y ejercer los derechos humanos, pero también para infringirlos, por ejemplo, controlando nuestros movimientos, compras, conversaciones y comportamientos.

5.1. Internet y la Sociedad: Éxitos y desafíos

Después de un siglo y medio de investigación e innovaciones, Internet quedó firmemente establecido como un recurso accesible para muchas personas y que ofrecía una amplia variedad de beneficios potenciales. Los usuarios tenían mayor acceso a todo tipo de información y los gobiernos y negocios disponían de una nueva plataforma para proporcionar información y servicios.

El comercio electrónico trajo consigo crecimiento económico, mayor amplitud de oferta para los consumidores y oportunidades para productores, que trabajaban en las áreas más desfavorecidas, de llegar a nuevos mercados. Una variedad de opciones de comunicación, desde el correo electrónico a elaboradas redes sociales, hacían más fácil a amigos y familias separados geográficamente estar en contacto, y a extraños formar “*comunidades virtuales*” en torno a intereses comunes.

Los organizadores de base adoptaron Internet como plataforma de activismo político y social y empezaron a emplearlo para movilizar respuestas masivas a desastres naturales y violaciones de derechos humanos. Usuarios de todas las edades saludaron a Internet como un medio de expresión personal y las nuevas aplicaciones ayudaron a democratizar la tecnología, posibilitando que el ciudadano de a pie generara y difundiera noticias, información, opinión y entretenimiento.

Sin embargo, llegado el siglo XXI son todavía muchos los desafíos a los que se enfrenta Internet. Los usuarios eran víctimas de prácticas abusivas como el spam (correo comercial no deseado), virus, usurpación de identidad y pirateo. Los expertos técnicos responden con soluciones que intentan minimizar estos peligros continuos diseñando sistemas anti virus, filtros, transacciones seguras y otras medidas.

Dentro de los medios de información y comunicación creados tecnológicamente, destaca particularmente la Internet, que en manos de personas inescrupulosas puede constituirse en un medio idóneo para cometer un sin número de delitos, bajo un manto de cierta impunidad.

El manejo indiscriminado de la información personal y profesional a través de las aplicaciones que utilizan Internet y especialmente las redes sociales es un grave inconveniente que pone a las personas y organizaciones en serios problemas cuando dicha información es utilizada con fines delictivos.

Hoy en día escapar al desarrollo de las TICs, incluso para el ciudadano común, resulta prácticamente imposible, dado que sus medios y herramientas han colmado la vida moderna: tener un teléfono celular y preferiblemente de tipo inteligente, como el caso de los Smartphones, más que un requerimiento actualmente es una necesidad. Para casi todos los ámbitos de la vida (familiar, profesional, empresarial o en el entorno de amistades, se han desarrollado aplicaciones tecnológicas que buscan facilitar la comunicación y la solución de problemas.

Resulta imposible desmerecer los avances de las TICs, los cuales han facilitado a las personas la comunicación, trabajo, mayor productividad y resolución de problemas; sin embargo, el ingente flujo de información y comunicación facilita nuevas formas de delincuencia que se desarrollan con una fisonomía propia que las aleja de las formas tradicionales de cometer delitos.

Por tanto, resulta claro que hablar de delitos informáticos y era digital son hechos concurrentes, pues tales delitos no podrían haberse dado, sin que se hubieran desarrollado los avances tecnológicos señalados.

Ligados a los medios informáticos y las tecnologías de la información, los delincuentes informáticos han visto en la red un medio idóneo para cometer delitos y crear nuevas formas de robos, señales estafas, etc., que dadas sus particularidades, esta Comisión de Justicia y Estructura del Estado, ha considerado pertinente incluirlas como nuevos tipos penales, así como también, adecuar todo pertinente a delitos informáticos con el fin de evitar todo tipo de violencia en el entorno digital.

5.2. Delitos informáticos: Características

“El delito informático implica una conducta delictiva que hace uso de un dispositivo informático, en primera instancia trató de encuadrar en este tipo de delitos a aquellos ya existentes como el robo, el hurto, la estafa, la calumnia, la pornografía infantil, etc.; sin embargo, la adición del elemento tecnológico en muchos casos desemboca en la configuración de nuevos delitos con características propias, los cuales deben ser debidamente tipificados para su sanción.” Luzuriaga (2017).⁶

A través de estos delitos se atacan diversos bienes jurídicos, entendiéndose que

⁶ Definición propia del autor Mayor Dr. Germán Luzuriaga H., Jefe de la Unidad Nacional de Ciberinteligencia y ex Jefe de Informática de la Dirección Nacional de Comunicaciones de la Policía Nacional del Ecuador, en su obra: Luzuriaga, G. (2017). Delitos informáticos: la virtual realidad. Quito: Offset Chávez. 232pp. ISBN: 978-9942-28-322.1.

no solo el patrimonio de las organizaciones y personas puede verse en riesgo sino también su honra, su integridad sexual, su integridad personal, etc. El atentado y restricción de derechos y libertades individuales pueden verse seriamente comprometidos, además el delito no sólo puede causar daño a una persona o entidad en particular sino hacer daño a todo un conglomerado social.

Para determinar las características del delito informático dejando de lado la concepción genérica que puede traer consigo el término, resulta imprescindible tomar contemplar el uso de Internet, dado que dentro del desarrollo de las nuevas TICs, es éste el medio del cual se ha valido el delincuente informático para cometer una amplia gama de sus delitos.

El desarrollo y servicios de internet han requerido la creación de un sinnúmero de herramientas y aplicaciones como la Web, que eventualmente es objeto de ataques por parte de delincuentes. La delincuencia cibernética ha concebido a la par también un cúmulo de herramientas y aplicaciones destinadas a vulnerar los sistemas informáticos, dañándolos, sustrayéndoles información, suplantándolos, etc.

Estas situaciones determinan un alto grado de complejidad para este tipo de delitos, que han puesto en una situación delicada a todas aquellas instituciones y profesionales que de una u otra manera se encuentran vinculados con la problemática, por ejemplo policías, fiscales, jueces, peritos, etc.

El delito informático se encuentra ligado ineludiblemente características que presente Internet, que vienen a caracterizarlo. La neutralidad que brinda la red a través de un entorno sin fronteras, sin duda brinda al delincuente informático la oportunidad de moverse en un ámbito de aparente impunidad que lastimosamente en muchos de los casos llega a concretarse cuando la persecución del delito se desvanece con leyes, sistemas judiciales y órganos de investigación que se encuentran limitados a un marco jurisdiccional definido; y si bien para el efecto se han suscrito convenios internacionales y existe la cooperación internacional adecuada, la misma se muestra insuficiente con relación a la envergadura del problema que puede fácilmente poner en conflicto

sistemas judiciales, cuando una conducta está en un país tipificada como delito y en otro no.

Cuando se habla de delitos informáticos, éstos se caracterizan porque las fronteras físicas no los detienen, su independencia geográfica es absoluta ya que la información puede generarse en un sitio y aparecer al otro lado del mundo de forma inmediata o en pocos segundos. Este tipo de delitos son transnacionales al igual que la Internet, de esto se valen los delincuentes para extender sus tentáculos por todo el mundo, más aún cuando frente al carácter transnacional del delito informático, la legislación y los sistemas judiciales del mundo no guardan el consenso necesario para una efectiva persecución haciendo que los espacios jurisdiccionales entren en conflicto y salga beneficiada la ciberdelincuencia o delincuencia informática.

El anonimato que brinda Internet se ve facilitado por características como la falta de identificadores seguros, la portabilidad y la ubicuidad. Aun cuando puede incluso resultar sencillo determinar la dirección de origen (IP), ello no basta pues se requiere necesariamente identificar plenamente a la persona autora del delito. Además, los delincuentes informáticos en procura de ocultar su identidad no hacen uso de redes públicas a la que el común de las personas accede sino que utilizan las redes oscuras donde el anonimato viene a ser no una característica, sino una condición.

Cuando se habla de un delito informático, se puede descubrir que la característica de ubicuidad entendida como la capacidad de estar presente en todas partes al mismo tiempo, es un verdadero rompecabezas cuando el delincuente, la víctima y los datos se encuentran en distintos países, siendo un hecho que los centros de datos que albergan los servidores pueden estar en lugares ocultos por tema de simple increíble seguridad, albergando información de una compañía como de un delincuente informático.

Este cúmulo de situaciones determinan que la persecución del delito y del delincuente informático sean difíciles, requiriéndose para el efecto la debida cooperación internacional que debe sustentada en instrumentos internacionales

vinculantes, pues de otra forma las buenas intenciones no pasan de ser eso.

Otra característica de este tipo de delitos es que continuamente se encuentran innovándose: *“las tecnologías de la información y comunicación evolucionan rápidamente, por lo que es de esperar que los delincuentes informáticos creen nuevas herramientas, medios y formas para perpetrar sus delitos”*.

El concepto de descentralización de la red, también caracteriza al delito informático, cuando no se permite la existencia de una autoridad central que controle, regule y establezca directrices respecto de las actividades que se llevan a cabo en el entorno de Internet. Esto sin duda beneficia al delincuente informático, aun cuando el carácter descentralizado mira como condicionamiento técnico y una característica esencial de la red que garantiza su independencia y la no injerencia de grupos de poder.

5.3. Delitos en instituciones financieras u otras entidades

Son variadas las modalidades de delitos informáticos que se vinculan con las actividades que realizan los bancos, entidades financieras o de cualquier otro tipo, mismas que se encuentran comprendidas en el ámbito del Código Orgánico Integral Penal (2014) y que no tienen que ver única y exclusivamente con aquellos delitos que afectan al derecho a la propiedad, sino también al derecho a la información, considerando que cualquier intrusión o interceptación de información ya constituye un delito aun cuando no exista un perjuicio económico inmediato.

Para Martínez (2015), las modalidades conocidas para la comisión de delitos informáticos que afectan a los clientes de la banca, y que han sido tipificadas en el COIP de Ecuador, son:

- a. **Phishing**⁷: En el COIP este delito está contemplado en el número uno del Art. 230.

(...) Arcilla citado por Salamea menciona que: “Según lo describe la Unión Internacional de Telecomunicaciones, el “*phishing*” es un acto que tiene por objeto lograr que la víctima revele información personal o confidencial. El término *phishing* se empleó inicialmente con la utilización de los correos electrónicos para “pescar” (en inglés *fish*) contraseñas y datos financieros en un mar de usuarios de internet. El empleo de la grafía “*ph*” se relaciona con las convenciones terminológicas de uso común en la piratería informática.”

Salamea comenta que para la realización del *phishing* se han creado programas de *spyware*, direccionados a hurtar contraseñas que la persona digita en su computador; pudiéndose utilizar para ello *backdoors* (virus creados para que el sujeto activo del delito ingrese directamente a la información que un computador tiene y la revise). Pueden estar insertos en correos electrónicos no deseados, mensajes instantáneos de *spam*, solicitudes falsas de amigos, etc.

- b. **Pharming**. - En el *pharming* el sujeto activo del delito clona una página institucional, por ejemplo de un entidad bancaria o de una compañía de comercio electrónico y el usuario de ésta ingresa sus datos para realizar una transacción sin conocer que es falsa. El *pharming* está contemplado en el número 2 del Art. 230 del COIP.
- c. **Cloning o skimming**: Mediante éste se duplican o clonan tarjetas, sin que tal hecho sea conocido por sus titulares, valiéndose de terceras personas como empleados de tiendas a quienes los autores les proveen de artefactos electrónicos para copiar toda la información de la banda magnética. Este delito en el actual COIP está contemplado en el número 3 del Art. 230.

⁷ El *phishing* es una técnica de ingeniería social que emplea el envío masivo de correos electrónicos *spam*, en nombre de una entidad financiera con la finalidad de obtener datos personales y financieros (principalmente aquellos asociados a claves de acceso), o de redirigir a los usuarios a una página web falsa de la entidad donde estos tengan que depositar sus datos.

5.4. Principales derechos constitucionales reconocidos o vulnerados

Con el desarrollo de las nuevas tecnologías de la información y la comunicación, son distintos los bienes jurídicos que pueden verse vulnerados a través de la perpetración de un delito informático, así lo determina el inusual e innovador comportamiento que muestran los delincuentes informáticos que día a día crean nuevas formas y modalidades de delitos, si bien muchos de ellos permanecen con el tiempo, la tecnología cambia y por ende la forma en que se cometen los delitos.

La Constitución de la República del Ecuador en su artículo 66 números 11, 18, 19, 20, 21, 26 y 28 reconoce y garantiza entre otros:

- El derecho a guardar reserva sobre sus convicciones.
- El derecho al honor y al buen nombre.
- El derecho a la protección de datos personales.
- El derecho a la intimidad personal y familiar.
- El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual.
- El derecho a la propiedad en todas sus formas.
- El derecho a la identidad personal y colectiva.

Asimismo, reconoce y garantiza de forma amplia los derechos de las personas a la información, a la propiedad, a la intimidad, o cualquier otro derecho que se vea comprometido en la consecución de los delitos informáticos.

Respecto del desarrollo de las nuevas TICs, el texto constitucional este artículo 16 número 2 reconoce como derecho de las personas el acceso universal a las tecnologías de la información y comunicación, reconocimiento que es ratificado y fomentado en el contexto de una comunicación plural y diversa, cuando el artículo 17 del texto constitucional determina que: *“El Estado fomentará la*

pluralidad y la diversidad en la comunicación, y al efecto: (...) 2. Creación y el fortalecimiento medios comunicación públicos, privados y comunitarios, así como el acceso universal a las tecnologías de información y comunicación en especial para las personas y colectividades que carezcan de dicho acceso o lo tengan de forma limitada”.

En el ámbito de la información y la comunicación el artículo 18 número 1, de la Constitución de la República se reconoce el derecho a la información de forma amplia al señalar que:

Todas las personas, en forma individual o colectiva, tienen derecho a:

1. Buscar, recibir, intercambiar, producir y difundir información veraz, verificada, oportuna, contextualizada, plural, sin censura previa acerca de los hechos, acontecimientos y procesos de interés general, y con responsabilidad ulterior.

Por tal razón, uno no puede publicar y decir lo que quiera a través de los medios digitales o internet, pues aquello tendrá sus consecuencias cuando lo que se dice es a través de un medio público, vulnerando el derecho de terceros a su intimidad, al buen nombre, etc., si bien la Constitución de la República en su artículo 66, el número 6 reconoce y garantiza las *personas “el derecho a opinar y expresar su pensamiento libremente y en todas sus formas y manifestaciones”*, este derecho encuentra su límite en el derecho de los otros.

En este sentido la Constitución de la República en el mismo artículo 66 reconoce y garantiza una amplia gama derechos individuales en relación a las libertades civiles, como son:

“(...) 4. Derecho a la igualdad formal, igualdad material y no discriminación.

18. *El derecho al honor y buen nombre. La Ley protegerá la imagen y la voz de la persona.*

19. *El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la Ley.*

20. *El derecho a la intimidad personal y familiar.*

21. *El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; ésta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la Ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen. Este derecho protege cualquier otro tipo o forma de comunicación.*

26. *El derecho a la propiedad en todas sus formas, con función y responsabilidad social y ambiental. El derecho al acceso a la propiedad se hará efectivo con la adopción de políticas públicas, entre otras medidas.*

28. *El derecho a la identidad personal y colectiva, que incluye tener nombre y apellido, debidamente registrados y libremente escogidos; y conservar, desarrollar y fortalecer las características materiales e inmateriales de la identidad, tales como la nacionalidad, la procedencia familiar, las manifestaciones espirituales, culturales, religiosas, lingüísticas, políticas y sociales.”*

5.5. Cooperación internacional

La legislación nacional bien concebida, instrumentos internacionales de cooperación convergen en la lucha contra los delitos informáticos contrarrestando un mal que puede poner en riesgo a la estructura social, dada la incidencia que hoy en día tienen las nuevas TICs en las actividades que realiza día con día el ser humano en su trabajo, en la empresa, en el hogar, con amigos, etc., llegando a ser una amenaza incluso para los Estados que pueden ver

comprometida su seguridad cuando son víctimas del ciberterrorismo o ciberespionaje.

Por tales motivos, son necesarios acuerdos internacionales el marco de respeto a los derechos humanos y a la soberanía de los medidas y alternativas que busquen erradicar este tipo de delitos informáticos y violencia digital

Tales acuerdos deben tener al menos un mínimo condicionamiento de obligatoriedad, pues caso contrario no dejan de constituirse en meras buenas intenciones.

Los mecanismos formales a nivel interno y en el ámbito del derecho internacional se muestran imprescindibles para que la asistencia y cooperación internacional se hagan realidad, en especial en ámbitos en los que las jurisdicciones de los distintos estados entran en conflicto y se constituyen en un obstáculo insalvable que solo trabaja en beneficio de la impunidad de los delincuentes informáticos.

5.6. Responsabilidad proveedores de internet

Característica común entre los países de Latinoamérica en cuanto a la responsabilidad de intermediarios en Internet por contenidos infractores, es la marcada ausencia de regulación en general, que tiende a revertirse recién a partir de la implementación de tratados de libre comercio. Esto se ve matizado por el desarrollo jurisprudencial, fundamentalmente a propósito de alegaciones de delitos contra la honra, y por iniciativas legales con éxito diverso motivadas por la protección de derechos de propiedad intelectual. Es decir, los esfuerzos de reformas a nivel normativo tienen una motivación diversa de los bienes jurídicos que más han sido esgrimidos para exigir la regulación legal de la responsabilidad de intermediarios. Algunos países merecen atención especial.

Los operadores de redes de telecomunicaciones y proveedores de acceso a una red de telecomunicaciones que presten un servicio de intermediación que consista en transmitir por una red de telecomunicaciones datos facilitados por el destinatario del servicio o en facilitar acceso a esta no serán responsables por la información transmitida, salvo que ellos mismos hayan originado la transmisión, modificado los datos o seleccionado estos o a los destinatarios de dichos datos.

No se entenderá por modificación la manipulación estrictamente técnica de los archivos que alberguen los datos, que tiene lugar durante su transmisión. Las actividades de transmisión y provisión de acceso a que se refiere el apartado, anterior incluyen el almacenamiento automático, provisional y transitorio de los datos, siempre que sirva exclusivamente para permitir su transmisión por la red de telecomunicaciones y su duración no supere el tiempo razonablemente necesario para ello.

Los operadores de redes disponen la infraestructura básica para la circulación de los datos en forma electrónica (cableado, satélites, nodos, entre otros). En la práctica, la mayoría de los operadores de telecomunicaciones son los tradicionales operadores de redes telefónicas, dado que el acceso a internet se realiza fundamentalmente a través de tales redes, aunque en los últimos años nuevos operadores han desarrollado redes propias de fibra óptica o redes inalámbricas (wifi). En la práctica también es habitual que los operadores de redes ofrezcan servicio de acceso a internet, e incluso servicios integrales de acceso, memoria caché, alojamiento de datos y transmisión de datos.

5.7. Violencia Sexual Digital en América Latina y el Caribe

Se han visto avances en los últimos años en los países de América Latina y el Caribe en la lucha contra la violencia en línea contra las mujeres. Con respecto a la legislación contra el “*porno vengativo*”, por ejemplo, se promulgó la Ley #

13.772/2018⁸ en diciembre de 2018 en Brasil, que modifica la legislación anterior para penalizar la grabación no autorizada y la exposición de contenidos desnudos o sexuales.

Dichos actos se están considerando ahora como “*violencia doméstica*” a los efectos de la Ley, en los casos en que hubo una relación preexistente entre la víctima y el autor. Los medios de comunicación tuvieron un papel crucial en el fomento del debate sobre el porno vengativo después de la ocurrencia de casos concretos.

Dichos debates llevaron a cambios legislativos que abordan directamente el problema (Neris et al., 2018). Argentina, Chile, México y Uruguay son ejemplos de Estados Miembros de la OEA que actualmente están discutiendo proyectos de Ley relacionados con el porno vengativo (Neris et al., 2018). México en particular ha propuesto una enmienda específica a su Código Penal y la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia⁹ que aborde el acoso cibernético contra las mujeres. (Cruz, 2019).

Además, varios países de América Latina han aprobado legislación sobre acoso político contra las mujeres (Bolivia) o están discutiendo proyectos de Ley relacionados (Costa Rica, Ecuador, Honduras, México y Perú) (OEA, 2017). Según lo descrito anteriormente, esto es crucial, entre otras razones, debido al impacto que tiene la tecnología en los debates democráticos.

En lo que respecta a la policía especializada en ciberdelito y/o violencia en línea contra las mujeres, también se han visto avances en los últimos años. México tiene una división de su servicio policial que se centra específicamente en el

⁸<https://www2.camara.leg.br/legin/fed/lei/2018/lei-13772-19-dezembro-2018-787488-publicacaooriginal-157031-pl.html>

⁹ Ley General de Acceso de las Mujeres a una Vida Libre de Violencia.

delito cibernético, atendiendo casos de violencia en línea¹⁰, además de un portal gubernamental en línea que tiene contenidos específicamente relacionados con la concientización sobre el acoso cibernético¹¹. En Brasil, algunos estados tienen departamentos de policía especializados, pero otros no¹². En Perú, cualquiera puede interponer una denuncia de violencia en línea a través de un formulario en línea, incluso si la persona que interpone la denuncia no es la víctima¹³.

Esta no es una revisión exhaustiva de lo que está sucediendo en los países de América Latina y el Caribe. Más bien, es una breve descripción destinada a demostrar la complejidad del problema. Es posible notar que los países se están moviendo hacia el reconocimiento y la definición del problema, así como al fortalecimiento de las protecciones para las mujeres en línea. Al mismo tiempo, están apareciendo nuevos métodos y tecnologías, y se están poniendo en práctica varias formas de violencia en línea todos los días.

5.8. Violencia en línea contra las mujeres

Aproximadamente la mitad de la población mundial está compuesta por mujeres (Banco Mundial, 2019), pero solo el 48% de ellas tiene acceso a Internet (en comparación con el 58% de los hombres) (UIT, 2019)¹⁴, y esta brecha digital se agrava aún más cuando se adopta una perspectiva transversal, p. ej. género y raza, etnia, discapacidad y edad. Esta grieta tiene implicaciones importantes en términos del empoderamiento y desarrollo de las mujeres, así como para las sociedades, las empresas y las economías. Además de las brechas en el acceso, la falta de habilidades en alfabetización digital sigue siendo una realidad para muchas mujeres.

¹⁰ <http://www.ssp.df.gob.mx/ciberdelincuencia.htm>

¹¹ <https://www.gob.mx/ciberbullying>

¹² <https://new.safernet.org.br/content/delegacias-ciber Crimes>

¹³ <http://www.noalacosovirtual.pe/>

¹⁴ Estas son cifras estimadas, ya que la mayoría de los países no le presentan a la Unión Internacional de Telecomunicaciones (UIT) datos desglosados por género (Web Foundation, 2018).

El concepto de alfabetización digital se refiere tanto a las habilidades técnicas que se necesitan, como a la capacidad de interactuar con los contenidos en línea de manera crítica (UNICEF, 2017). Además, la GSMA (2015) ha encontrado, por ejemplo, que muchas mujeres en países en desarrollo no comprenden la profundidad y amplitud de lo que podría ofrecerles el Internet en términos de contenido, ya que están atrapadas en unas “*islas de aplicativos*”, o sea que, lo que entienden como el “*Internet*” es lo que ven a través de un cierto número de aplicativos móviles. Contar con habilidades adecuadas de alfabetización digital es clave, en especial si se tiene en cuenta que el acceso y el uso de Internet han creado incontables posibilidades que nunca hubiéramos imaginado. Ha afectado profundamente cómo nos comunicamos, cómo accedemos a la información y cómo entendemos nuestras propias identidades.

Al no tener una alfabetización adecuada, las mujeres no son plenamente conscientes de los riesgos que corren con el uso de Internet. De hecho, a pesar de la extensa gama de oportunidades que brinda, la adopción y el uso de Internet también se han visto acompañados por desafíos como la necesidad de fortalecer la privacidad y la seguridad, ya que nuestras vidas se desarrollan cada vez más a través de nuestras identidades en línea. Un ejemplo de cómo las mujeres pueden exponerse en línea involuntariamente es con las filtraciones de datos. En la India en 2019, más de 12 millones de registros médicos relacionados con la salud reproductiva de las mujeres, alojados por una agencia gubernamental, fueron expuestos en línea. El problema fue abordado por el Equipo nacional de respuesta a emergencias informáticas (CERT) en cooperación con un investigador extranjero, pero tardó semanas en resolverse (Cimpanu, 2019). La exposición de la información personal de las mujeres es en sí misma una violación de su derecho a la privacidad, pero también las hace más susceptibles a sufrir diferentes tipos de acoso y violencia en línea.

Todavía no existe acuerdo sobre una definición de la multiplicidad de comportamientos que constituyen la “*violencia en línea*” contra las mujeres, aunque comúnmente se dice que son los comportamientos en contra de una mujer en particular. Puede ser, por ejemplo, cuando una mujer recibe un mensaje directo a través de Internet o se difunde su información a través de Internet sin

su consentimiento, lo que puede generar una infinidad de sentimientos negativos y traumáticos (PRC, 2018). Dada la importancia actual del tema y la creciente demanda de un marco legal y regulatorio para abordar de manera más efectiva la violencia en línea contra las mujeres, las y los asambleístas miembros de esta Comisión de Justicia y Estructura del Estado, han trabajado arduamente en el tratamiento y análisis del presente proyecto de Ley, con el que se pretende aportar a combatir todo tipo de violencia en el entorno digital y delitos informáticos.

5.9. Interseccionalidad

La interseccionalidad es una herramienta analítica que reconoce que las desigualdades sistémicas se configuran a partir de la superposición de diferentes factores sociales como el género, la etnia y la clase social. En consecuencia, tanto las desventajas como los privilegios que tiene una persona en un momento y lugar determinados no pueden entenderse examinando de forma aislada los diversos elementos de su identidad. Por el contrario, se debe prestar atención al conjunto de relaciones de poder que le afectan, incluidas aquellas fuerzas a nivel macro como el pasado colonial y la pobreza; y las fuerzas a nivel micro, entre ellas el estado de salud de una persona y la estructura de su familia o comunidad.¹⁵

La interseccionalidad puede ser aplicada tanto para el análisis jurídico y de políticas públicas, así como en la incidencia y las metodologías de investigación. Su valor analítico radica en visibilizar las diferencias entre mujeres, hombres o cualquier otro grupo de personas y, a su vez, toma en cuenta los efectos de los sistemas de discriminación como el sexismo, el racismo y el clasismo.

La interseccionalidad permite identificar cómo las iniciativas legislativas propuestas tendrán un impacto positivo o negativo en diferentes individuos y grupos sociales. Además, garantiza que las leyes y las políticas públicas sean diseñadas de manera tal que las diversas experiencias de quienes integran la

¹⁵ Extracto de Interseccionalidad, ParlAmericas.:
https://parlamericas.org/uploads/documents/Intersectionality_es.pdf

población nacional sean incluidas, evitando así el pensamiento y soluciones únicas, con el objetivo de que tales leyes y políticas públicas tengan un carácter más receptivo y eficaz para el beneficio del mayor número de personas posible. La visión y perspectiva matizada proporcionadas adicionalmente por la consulta extensiva y el análisis interseccional promoverán un mejor servicio de atención a la ciudadanía.

Asimismo, la Ley Orgánica Integral para Prevenir y Erradicar la Violencia Contra las Mujeres¹⁶, define al enfoque de interseccionalidad como aquel que *“identifica y valora las condiciones sociales, económicas, políticas, culturales, religiosas, étnicas, geográficas, físicas y otras que son parte simultánea de la identidad individual y comunitaria de las mujeres y adecúa a estas realidades las acciones, servicios y políticas públicas destinadas para la prevención y erradicación de la violencia contra las mujeres y la atención, protección y restitución de derechos de la víctima.”*

La interseccionalidad revela las limitaciones en el uso de "mujer" y "hombre" como categorías de análisis cerradas u homogéneas, resaltando la diversidad que existe al interior de los grupos sociales que, de otro modo, podría ser ignorada.

5.10. Sexualización del cuerpo de la mujer

Para darnos una idea sobre la sexualización del cuerpo de la mujer, debemos tener en cuenta que este tipo de sexualización lo que hace es cosificar a la mujer de una forma sexual, pero ¿qué es cosificar?

La cosificación sexual según Bartky *“es la reducción de una mujer en su cuerpo o partes de éste con la percepción errónea de que su cuerpo o partes del mismo pueden representarla en su totalidad”* (Bartky, 1990). La cosificación sexual es

¹⁶ Ley Orgánica Integral para Prevenir y Erradicar la Violencia Contra las Mujeres. Art. 7 Enfoques: f) Enfoque de interseccionalidad.

vista como una forma un tanto sutil de discriminación sexista, pero no por ello es menos grave.

La sexualización del cuerpo tiene mayor relevancia entre las mujeres que entre hombres. Las mujeres están expuestas cotidianamente a eventos sexistas de todo tipo. Por ejemplo, la sociedad aún tiene el pensamiento de que las mujeres construyen su cuerpo para ser mirado, y esto es algo inaceptable hoy por hoy.

La *Teoría del Sexismo Ambivalente* formulada por Glick y Fiske (1996), resalta la idiosincrasia del prejuicio contra las mujeres, debido a los sentimientos positivos que existen hacia ellas y que coexisten con sentimientos negativos, hostiles o de rechazo.¹⁷

Si bien es cierto la sexualización de la mujer tiene su origen en aquellas estructuras simbólicas patriarcales que definen a las mujeres como naturaleza, biología y sexo, y en aquellas estratificaciones sociales que subordinan, interiorizan y devalúan a las mujeres.¹⁸

En las últimas décadas, los medios de comunicación han avanzado en la producción de imágenes de mujeres hipersexualizadas. Este tipo de imágenes reducen el cuerpo de la mujer a un atractivo sexual que llame la atención, y el éxito que tienen estas imágenes es que éstas se articulen en torno a la reproducción de las mujeres como seres sexuales para los varones.

La sexualización del cuerpo de la mujer en los medios de comunicación se manifiesta especialmente a través de la vestimenta y de las posturas que adoptan los diferentes modelos. Esto se puede apreciar desde la perspectiva de Fredrickson y Roberts, puesto decían que: *“los medios de comunicación son el vehículo principal para la cosificación de la mujer en las culturas occidentales”*.¹⁹

¹⁷ Glick, P. y Fiske, S. T. (1996). The Ambivalent Sexism Inventory: Differentiating hostile and benevolent sexism. *Journal of Personality and Social Psychology*, 70, 491-512.

¹⁸ Coral, A. (2010). El cuerpo femenino sexualizado: entre las construcciones de género y la Ley de Justicia y Paz. *International Law*, (17), 381-409.

¹⁹ Fredrickson, B. L. y Roberts, T. A. (1997). Objectification theory: Toward understanding women's lived experiences and mental health risks. *Psychology of Women Quarterly*.

Si nos ponemos a pensar, la sexualización del cuerpo de la mujer tiene un trasfondo eminentemente patriarcal, dado que las mujeres son vistas como objetos en lugar de sujetos desde la visión patriarcal. El patriarcado mira a las mujeres desde una perspectiva sexual, en donde estás deben estar al servicio del poder masculino. Hoy en día, aunque no parezca cierto, este discurso cuyo ánimo es denigrar a las mujeres y ponerlas en una posesión de inferioridad, lamentablemente aún existe en nuestra sociedad y es cada día más reproducido y normalizado.

Ahora bien, las relaciones Derecho-Estado con las mujeres presentan un campo un tanto difícil de navegar, ya que confluye con un “*derecho masculino*” en donde los cuerpos sexualizados y marginados se explican sobre la base de una ordenación biológica y natural.

La percepción visual del cuerpo sexualizado es muy similar a como una persona visualiza y percibe un objeto. Cognitivamente, percibimos partes del cuerpo, no vemos una imagen global. Por ejemplo, si vemos una mujer con un amplio escote y pechos prominentes es probable que nos centremos en eso. No es difícil imaginarse que si tenemos que describirla diríamos (o pensáramos) “*la de los pechos grandes*”.²⁰ Si percibimos el cuerpo de las mujeres como objetos les atribuimos menos rasgos típicamente humanos.

La sexualización del cuerpo de la mujer no solo es percibida en su etapa adulta, sino que es percibido tanto en niñas y adolescentes. El profesor Víctor Grande López, en el año 2019 mencionó en su obra: “*La hipersexualización femenina en los medios de comunicación como escaparate de belleza y éxito*” que: “*La obsesión por el cuerpo puede llevar a una persona a no sentirse bien, afectando negativamente en su autoestima. Una preocupación muchas veces derivada de pequeños detalles que logran masificarse en las percepciones internas de la persona; es el conocido como trastorno dismórfico corporal, poco estudiado y es*

²⁰<https://www.comportamientonoverbal.com/clublenguajenoverbal/cosificacion-y-deshumanizacion-a-traves-de-vestimenta-y-posturas-sexualmente-sugestivas-club-de-lenguaje-no-verbal/>

*necesario exponerlo en al ámbito educativo para trabajarlo desde edades tempranas*²¹.

Un ejemplo claro de sexualizar el cuerpo de la mujer, como se dijo en líneas anteriores, es por su forma de vestir. Ante esto la Corte Constitucional del Ecuador en la sentencia 751-15-EP/21²², en donde se habla acerca de los estereotipos de vestimenta que promueven un trato desigual hacia las mujeres dictaminó que:

- *“Existe vulneración del derecho a la igualdad y no discriminación ya que esto constituye una medida discriminatoria que no tiene justificación alguna; se basa en patrones estereotipados de comportamiento que promueven un trato desigual hacia las mujeres.*
- *Se declaró la vulneración al libre desarrollo de la personalidad, cuando autoridades de un Centro de Rehabilitación Social consideraron como “corto” un vestido que llevaba puesto una abogada que pretendía ejercer su profesión en defensa de respuestas motivadas, a la cual le impidieron el acceso”.*

Como se puede apreciar, la sexualización del cuerpo de la mujer ocurre día a día y muchos casos como el que sentenció la Corte Constitucional quedan en la impunidad. Debemos ser más conscientes y responsables sobre nuestras percepciones hacia las mujeres, el hecho de que una mujer se vista con la ropa que quiera no quiere decir que la tengamos que sexualizar o que esté buscando que se le agrede o violente.

De igual forma, todos somos parte del problema y debemos ser parte de la solución, debemos combatir este problema desde la raíz para que se erradiquen

²¹ CP, 2019, Vol.8 – No16, pp. 21/32 ISSN 2014-6752. Girona (Catalunya). Universitat de Girona. GRANDE-LÓPEZ, Víctor: La hipersexualización femenina en los medios de comunicación como escaparate de belleza y éxito. Recibido: 15/04/2019 - Aceptado: 01/07/2019

²²http://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/e2NhenBldGE6J3RyYW1pdGUnLCBldWlkOic0NTZkYzFmMS01YmMwLTRjOWEtOWMxOS1iNTM0Mzg5OTUxNWlucGRmJ30=

este tipo de inconductas y podamos vivir en una sociedad libre de discriminación y sexualización hacia la mujer.

La cosificación sexual de la mujer nos arroja la conclusión de que mientras la sociedad siga cosificando a la mujer y a su cuerpo, se mantendrán las ideas de subordinación femenina, aumentando el sexismo benévolo²³ y debilitando la acción colectiva de las mujeres contra el patriarcado.

Caso tenista Alize Cornet sancionada

- Un ejemplo de impacto mundial en el Abierto de Estados Unidos del 2018 la tenista francesa Alize Cornet regresó del cambio de vestuario con la camiseta al revés, al percatarse se sacó para ponérsela correctamente y debajo tenía un top deportivo esta justa de vestimenta le mereció una advertencia por conducta antideportiva mientras que los jugadores libremente se sacan la camiseta en la cancha sin ningún tipo de amonestación eso se llama doble estándar.
- Alize Cornet se encontraba jugando en las canchas Flushing Meadows, en la ciudad de Nueva York.
- Ese día Nueva York tenía una temperatura de casi 40 grados.
- En el duelo que tenía Cornet, estaba la “*regla de calor*”.
- El objetivo de la “*regla de calor*” es proteger a los jugadores durante temperaturas extremas y permite, en el caso de las mujeres, una pausa de 10 minutos para refrescarse e hidratarse después del segundo set.
- Cornet al volver de la pausa de 10 minutos para jugar el tercer set, la tenista se percató que se había puesto la camiseta al revés.
- Alize Cornet decidió quitarse la camiseta, le dio la vuelta y se la volvió a poner.
- El cambio fue breve. Y lo único que dejó a la vista fue un sujetador deportivo negro.

²³Glick y Fiske (1996) describen el sexismo benévolo como un conjunto de actitudes sexistas hacia las mujeres, las cuales son concebidas estereotípicamente y restringidas a ciertos roles, pero que tiene un tono subjetivamente positivo y tiende a provocar conductas típicamente categorizadas como prosociales o de búsqueda de intimidad. Obtenido en el siguiente link: <http://www.scielo.org.co/pdf/sumps/v22n2/v22n2a01.pdf>

- Este simple ajuste de vestimenta, le costó a la tenista una advertencia por parte del *umpire* Christian Rask debido a que la acción es considerada una violación del código de conducta deportiva.
- Esta decisión causa una gran polémica, sobre todo por el agravio comparativo, ya que los hombres pueden hacerlo sin recibir ningún tipo de amonestación.
- Cornet en rueda de prensa declaró: *“Claro que tomó por sorpresa cuando me cambié la camiseta bien rápido y me señaló la infracción (...) Era algo que me lo esperaba y le dije que fue algo muy raro”*.
- Horas antes de esta rueda de prensa, la Federación de Tenis de Estados Unidos emitió un comunicado en el que lamentan que Cornet fue sancionada.
- Este comunicado decía *“Hemos aclarado la norma para asegurar que esto no vuelve a ocurrir en el futuro”*.
- El US Open indicó que todos los jugadores pueden cambiar de camiseta en sus sillas y mencionó que las mujeres pueden cambiarse la camiseta en un *“lugar más privado”* cerca de la cancha sin tener que ceder una de las pausas para ir al baño que disponen.
- ¿Por qué hablamos de que las mujeres deben cambiarse en un lugar más privado?
- El circuito femenino de tenis, la WTA, calificó de *“injusta”* la advertencia y recordó que no tienen una norma que prohíba lo hecho por Cornet.

5.11. Doble estándar

En la sociedad contemporánea, se cree que las mujeres deben estar sujetas a estándares diferentes de comportamiento sexual que los hombres. Por este motivo, surge el término doble estándar sexual, el cual consiste en *“evaluar los mismos comportamientos sexuales en hombres y mujeres usando diferentes criterios”* (Álvarez, Gómez, Sierra, 2020, p.1). Esto genera que la valoración de la conducta sexual femenina sea más restrictiva que la masculina.

El doble estándar sexual es un problema que debe ser analizado y atendido, ya que según Monge (2013) *“la presencia de un doble estándar sexual incrementa el riesgo de sufrir violencia de pareja”*. Esta afirmación se relaciona íntimamente con el aumento significativo de la violencia contra la mujer en los últimos años. Sin embargo, este tema ha sido analizado como violencia en contra de la mujer, por lo que resulta imprescindible incorporar este tema con el doble estándar sexual.

De acuerdo con el doble estándar sexual, los niños y los hombres son recompensados y elogiados por sus contactos sexuales heterosexuales, mientras que las niñas y las mujeres son derogadas y estigmatizadas por comportamientos similares²⁴. Un estudio realizado en Latinoamérica calculó que alrededor de 5% de las víctimas adultas de la violencia sexual notificaron el incidente a la policía, esto se debe a que en muchos de los casos no llegan a salir a la luz pública, debido a la vergüenza, miedo de ser culpadas, miedo a las represalias y a un sistema de apoyo inadecuados (Organización Panamericana de la Salud, 2013)

El doble estándar sexual puede explicarse con tres teorías según Zaikman y Marks (2017). Para lo cual, plantea la teoría evolutiva, misma que sugiere que las adaptaciones evolutivas influyen en la forma de observar las conductas sexuales de otras personas y las propias, por lo que ciertos rasgos de comportamiento son vistos como una ventaja de supervivencia. La segunda teoría es la del rol social, la que postula que el doble estándar sexual ocurre porque la sociedad tiene diferentes expectativas en lo referente al comportamiento de los hombres y de las mujeres. Finalmente, la teoría del aprendizaje social cognitivo de Bandura dice que el doble estándar sexual existe por el refuerzo y castigo que se dan a los comportamientos consistentes con los roles de género.

Del doble estándar se deriva también el doble estándar moral sexual. Esto también se relaciona con el uso de la agresividad e incluso la violencia por parte

²⁴ <https://journals.sagepub.com/doi/abs/10.1177/019027250907200205>

del hombre hacia la mujer, lo cual forma parte del machismo o la hipermasculinidad (Mosher y Sirkin, 1984). Lo antes mencionado demuestra que las mujeres son las más perjudicadas por este doble estándar.

García y Cabello (2013) señalan que, si bien los hombres y las mujeres son más parecidos que opuestos, todavía existen ideas erróneas sobre las características típicamente masculinas o femeninas, por ejemplo, la idea de que la mayoría de los hombres son infieles o que todas las mujeres son hipersensibles. Estas ideas se presentan en los diferentes ámbitos de la cultura humana, encontrando por ejemplo un fuerte impacto en el ámbito educativo, tal como se expresa en las discusiones correspondientes al enfoque de género.

A partir de lo antes mencionado, se puede considerar que el enfoque de género crea varias actitudes que por lo general están relacionadas con la doble moral sexual. Esta doble moral relacionada a la sexualidad se pone de manifiesto cuando se dice que se respeta la libertad de hombres y mujeres, pero al momento de hablar de una mujer que tenga una vida sexual activa se considera que no es una mujer con la cual se mantendría una relación seria o estable, aunque si esto se ve en un hombre es celebrado por familiares y amigos.

Un claro ejemplo de lo anteriormente citado, es que las mujeres que mantienen una relación monogámica son menos juzgadas que las que tienen múltiples parejas o hijos con diferentes padres. Otro ejemplo, es cuando en una pista de baile están dos hombres y evitan bailar entre ellos, porque podría indicar homosexualidad, pero si dos mujeres están bailando entre ellas no se consideraría lesbianismo. El doble estándar sexual también ha cambiado los conceptos culturales para lograr posicionarse de un modo diferente en la sociedad.

Como hemos visto el doble estándar sexual afecta en mayor medida a las mujeres, las cuales deben continuar actuando como la sociedad lo ha definido y si llegan a romper esta norma social como diría Durkheim, son juzgadas y reciben una penalización ante esto. Por lo cual, es necesario que las leyes

respalden a las mujeres y no sean penalizadas por realizar acciones que en el caso de los hombres no serían castigadas con esa severidad.

El Derecho en estos casos no se encuentra ni solo ni aislado, sino que ha recibido influencias sociales, culturales, históricas y políticas que llegan a afectar el acceso a la justicia. Si se producen situaciones que afecten a estos elementos anteriormente mencionados con certeza se verá afectado el acceso a la justicia (Álvarez, pp.29-31). Por este motivo, sería conveniente que para el juzgamiento de un delito relacionado al doble estándar se implementen una normatividad que logre sistematizar las conductas con el fin de prevenir acciones punibles que normen que es lo que se debe hacer o no en la vida social.

Se puede concluir que el doble estándar sexual abre el camino a un doble estándar moral, lo que significa que para ciertos grupos de la sociedad esta correcto alguna situación mientras que para otro será totalmente erróneo. Además, que estos conceptos están íntimamente relacionados con los aspectos culturales y sociales que determinan lo bueno y malo del accionar de las personas en lo inherente a la sexualidad. A la vez, que en gran medida afecta a las mujeres generando normas sociales más restrictivas de comportamiento, a diferencia de los hombres.

6. NORMATIVA INTERNACIONAL

6.1. Convención Americana sobre Derechos Humanos

Mediante la Convención Americana sobre Derechos Humanos, el Ecuador se comprometió con tres grandes ejes: con la construcción de la democracia, la libertad personas y la justicia social, ejes que se fundamentan en la igualdad de las personas, ante la Ley.

De tal manera, en el artículo 5, número 1, de dicha Convención, se establece que “(...) *toda persona tiene derecho a que se respete su integridad física,*

psíquica y moral (...).²⁵ De igual manera, la Convención, en su art. 7, número 1, instituye que “(...) *toda persona tiene derecho a la libertad y a la seguridad personales (...)*”.²⁶ Asimismo, el art. 11, número 2, del instrumento en cuestión, establece que “(...) *nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación (...)*”.²⁷ Finalmente, el número 3, del art. 11, menciona que “(...) *toda persona tiene derecho a la protección de la Ley contra esas injerencias o esos ataques (...)*”²⁸

En este sentido, nuestro país se comprometió en garantizar la igualdad de derechos para todos sus ciudadanos, asegurando así una vida digna en todos los ámbitos. Además, de manera particular, la Ley debe proteger a las personas, para que no sufran ningún tipo de injerencia, que atente contra la integridad física, psicológica o sexual. Por ello, es indispensable avanzar hacia normas modernas, que consideren los fenómenos propios de la globalización y el avance tecnológico.

6.2. Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer

A través de este instrumento, el Ecuador se comprometió por trabajar por la eliminación de la violencia, tanto en el ámbito público como en el privado. Por su lado, los Estados parte reconocieron que la violencia contra las mujeres constituye una grave violación de los derechos humanos y las libertades fundamentales y, a su vez, limita total o parcialmente el reconocimiento, goce y ejercicio de tales derechos, recogido en los instrumentos internacionales. Igualmente, se determinó que toda forma de violencia de género constituye una ofensa a la dignidad humana y una manifestación de las relaciones de poder existentes entre hombres y mujeres, mismas que han sido históricamente institucionalizadas y aprobadas por la sociedad.

²⁵ Convención Americana sobre Derechos Humanos, 1969.

²⁶ *Ibidem*.

²⁷ Convención Americana sobre Derechos Humanos, 1969.

²⁸ *Ibidem*.

En ese sentido, el artículo 1, de la Convención, define la violencia contra la mujer como “(...) cualquier acción o conducta, basada en su género, que cause muerte, daño o sufrimiento físico, sexual o psicológico a la mujer, tanto en el ámbito público como en el privado.”²⁹ Bajo dicha conceptualización, los Estados parte asumieron principalmente cuatro compromisos: “1. Actuar con debida diligencia para prevenir, investigar y sancionar toda forma de violencia contra las mujeres; 2. Desarrollar normas jurídicas armoniosas con los objetivos de la Convención y, mediante ellas, garantizar el acceso a la justicia, el acompañamiento psicológico y la no revictimización de la mujer; 3. Desarrollar planes y proyectos educativos que tiendan a modificar los patrones socioculturales de conducta de hombres y mujeres, eliminando estereotipos sobre hombres y mujeres; y, 4. Implementar planes de capacitación para los agentes policiales y los funcionarios judiciales, para que dejen de minimizar el fenómeno de la violencia de género.”

6.3. Aplicación de recomendaciones efectuadas mediante la Observación General No. 25 sobre los derechos del niño en relación con el entorno digital

Esta Comisión, insiste mediante el presente documento, en que los derechos de todos los niños deben ser respetados, protegidos y cumplidos en el entorno digital. Como se ha mencionado ya a lo largo del tratamiento del presente proyecto de Ley, el acceso significativo a las tecnologías digitales puede ayudar a los niños a realizar toda la gama de sus derechos civiles, políticos, culturales, económicos y sociales, sin embargo, si no se logra la inclusión digital, es probable que aumenten las desigualdades existentes y que surjan otras nuevas.

Los delincuentes sexuales pueden utilizar tecnologías digitales para solicitar a los niños con fines sexuales y participar en el abuso sexual infantil en línea, por ejemplo, mediante la transmisión de video en vivo, la producción y distribución de material de abuso sexual infantil y mediante la extorsión sexual. Las formas de violencia y explotación y abuso sexuales facilitados digitalmente también pueden perpetrarse dentro de un niño.

²⁹ Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer, 1994.

El círculo de confianza, por parte de familiares o amigos o, para los adolescentes, por parejas íntimas, y puede incluir la ciber agresión, incluido el acoso y las amenazas a la reputación, la creación no consensuada o el intercambio de texto o imágenes sexualizados, como contenido autogenerado. mediante sollicitación y / o coerción, y la promoción de conductas autolesivas, como cortarse, conductas suicidas o trastornos alimentarios. Cuando los niños hayan llevado a cabo tales acciones, los Estados partes deben aplicar enfoques de justicia preventiva, de salvaguardia y reparadora para los niños involucrados siempre que sea posible.

El Ecuador, por intermedio de esta Asamblea Nacional, cumplirá con lo determinado en este instrumento internacional, que determina que: *“Los Estados partes deben tomar medidas legislativas y administrativas para proteger a los niños de la violencia en el entorno digital, incluida la revisión periódica, la actualización y el cumplimiento de marcos legislativos, reglamentarios e institucionales sólidos que protejan a los niños de los riesgos reconocidos y emergentes de todas las formas de violencia en el entorno digital. Dichos riesgos incluyen violencia física o mental, lesiones o abuso, negligencia o maltrato, explotación y abuso, incluidos la explotación y el abuso sexuales, la trata de niños, la violencia de género, la ciber agresión, los ataques cibernéticos y la guerra de información. Los Estados partes deben implementar medidas de seguridad y protección adecuadas para los niños que están en constante evolución”.*

6.4. Adecuaciones para impulsar la Adhesión del Ecuador al Convenio de Budapest

Conforme el compromiso adquirido por las y los legisladores miembros de esta Comisión en el tratamiento para Primer Debate del presente proyecto de Ley, se propone un texto de articulado que realiza las adecuaciones necesarias en nuestra normativa penal, siguiendo las recomendaciones realizadas en un inicio por Cancillería, a efectos de impulsar la Adhesión del Ecuador al Convenio de

Budapest, demostrando así la voluntad política de esta Asamblea Nacional para combatir la violencia digital y la ciber delincuencia.

Dicho Convenio internacional trata sobre delitos cometidos a través de internet y otras redes informáticas, se ocupa especialmente de las infracciones de los derechos de autor del fraude informático, de la pornografía infantil y de las violaciones de la seguridad de la red. El objetivo principal de este instrumento es establecer una política penal común orientada a la protección de la sociedad contra la ciberdelincuencia, que se logra tipificando los delitos informáticos de forma similar en todas las naciones, unificando normas procesales y a través de una cooperación internacional.

En lo que respecta a la adhesión al Convenio de Budapest, el Artículo 37 señala lo siguiente: *"7. Después de entrar en vigor el presente Convenio, el Comité de Ministros del Consejo de Europa podrá, tras consultar a los Estados firmantes del Convenio y habiendo obtenido el asentimiento unánime de los mismos, invitar a todos los Estados no miembros del Consejo de Europa que no hayan participado en la elaboración del mismo a adherirse al Convenio. Esta decisión deberá tomarse mediante la mayoría prevista en el artículo 20.d del Estatuto del Consejo de Europa y el asentimiento unánime de los Estados firmantes que tengan derecho a formar parte del Comité de Ministros"*, sin embargo, con la presente reforma esta Asamblea Nacional del Ecuador, dejaría ya cumplido este paso, al dotar al país de una normativa lista y armonizada a dicho Convenio, para que así el próximo Gobierno quede comprometido con este proceso a fin de que se avancen con los demás pasos pertinentes para formalizar con éxito esta adhesión.

7. DIFERENTES TIPOS DE VIOLENCIA EN EL ENTORNO DIGITAL

Tras el análisis y procesamiento de absolutamente todas las observaciones y aportes que han sido presentados por diversos actores ante esta Comisión, ya sea de manera verbal en el Pleno, por escrito, o a través de las múltiples

comparecencias de expertos nacionales e internacionales en la materia, se ha podido identificar que existen al menos 20 diferentes tipos de violencia en el entorno digital que requieren ser reconocidos, adecuados y tipificados en nuestro Código Orgánico Integral Penal de manera urgente, a efectos de garantizar la máxima protección y prevención posible de toda la ciudadanía ante el posible cometimiento de estas inconductas que tienen las mismas o inclusive peores repercusiones que los tipos penales existentes, ya que sus secuelas son casi imborrables por la naturaleza del medio en el que se desarrollan.

Los miembros de esta Comisión consideran pertinente, recordar no solo al Pleno de esta Asamblea Nacional, sino a todas las y los ecuatorianos, que **“lo virtual es real”** y puede traer consecuencias irreparables en las víctimas, por lo que a continuación se detallan cada uno de estos diferentes tipos de violencia en el entorno digital que se los ha incluido en el texto propuesto para Segundo Debate:

7.1. *Grooming*:

El *“Grooming”* no es parte de la terminología de nuestro ordenamiento jurídico, sino que se trata más bien de una expresión anglosajona usada para describir un nuevo fenómeno criminológico.

La expresión *“Grooming”* o *“Child grooming”*, conforme el uso dado por los ingleses, consiste en aquellas acciones dolosas que adopta un adulto para crear una relación de confianza con un menor, con la intención de mantener contacto sexual con este.

El *grooming* es el proceso por el cual una persona prepara a un niño o niña, al adulto significativo y al entorno para el abuso de éste niño. Los objetivos específicos incluyen el ganar acceso al niño su complicidad y que el menor mantenga el secreto con el fin de evitar revelaciones. Este proceso sirve para

fortalecer la conducta abusiva del abusador, así como justificar y denegar sus acciones.³⁰

Este es uno de los pocos, por no decir casi el único tipo de violencia digital, actualmente reconocido en el COIP³¹ en el artículo 173 denominado “*Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos*”, de la siguiente manera:

“Art. 173.- Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos.- *La persona que a través de un medio electrónico o telemático proponga concertar un encuentro con una persona menor de dieciocho años, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento con finalidad sexual o erótica, será sancionada con pena privativa de libertad de uno a tres años.*

Cuando el acercamiento se obtenga mediante coacción o intimidación, será sancionada con pena privativa de libertad de tres a cinco años.

La persona que suplantando la identidad de un tercero o mediante el uso de una identidad falsa por medios electrónicos o telemáticos, establezca comunicaciones de contenido sexual o erótico con una persona menor de dieciocho años o con discapacidad, será sancionada con pena privativa de libertad de tres a cinco años.”

Dentro de este contexto, el *grooming* viene a ser una subespecie de acoso en la que ya no actúan pares pues implica la participación de un adulto hacia una niña, niño o adolescente. Para ello, el delincuente se vale de su condición por diversos medios en la red para, en primera instancia, lograr un contacto con el menor, luego ganar su confianza buscando controlarlo, someterlo y abusar de él, física

³⁰ Craven, S, Current responses to sexual grooming: Implication for prevention. The Howard Journal of Criminal Justice, citado en Pulido Rodríguez, Cristina, Prevención de abusos sexuales a menores en internet: Acciones preventivas online en España, Tesis, Universidad de Barcelona, 2006, p. 54.

³¹ Código Orgánico Integral Penal.

o sexualmente, abuso sexual que puede eventualmente conllevar a la configuración de otro delito como la pornografía infantil.³²

Caso Tik tok niña Medellín acosada desde Ecuador

- En septiembre del año anterior (2020), un video de una denuncia que realizó una joven colombiana se viralizó en redes sociales. Se trata de Carolina Hernández quien contó como su hermana fue contactada por una red de pedofilia. La joven expuso los mensajes de WhatsApp y el número tenía el código de Ecuador +593.
- Todo comenzó cuando su hermana de 8 años de edad siguió a la cuenta @karolsevilla_luna2 (la protagonista de la serie de Disney 'Soy Luna'), y esta también la siguió. Desde el perfil comenzaron a enviarle mensajes haciéndole preguntas personales, además de invitarla a participar en el concurso que consistía en cinco retos y cinco preguntas.
- La persona que se comunicaba con la niña le dijo que no le mencione nada a su familia. Sin embargo, la hermana de Carolina decidió contarle a su familia. Los cuales, se contactaron rápidamente con la Policía de la ciudad y armaron un perfil falso de una niña de 10 años. Tal como lo esperaban, esta persona se contactó con ella para decirle lo del concurso que consistía en hacer retos. Primero que responda preguntas como los nombres de sus mascotas y luego que le envié fotos de su cuerpo, en ropa interior, que se ponga en cuatro y exhiba sus partes íntimas.
- La Policía de la capital antioqueña anunció la apertura de una investigación con colaboración internacional para esclarecer quiénes están detrás de esa red criminal.

³² Código Orgánico Integral Penal: “Art. 103.- Pornografía con utilización de niñas, niños o adolescentes.- La persona que fotografíe, filme, grabe, produzca, transmita o edite materiales visuales, audiovisuales, informáticos, electrónicos o de cualquier otro soporte físico o formato que contenga la representación visual de desnudos o semidesnudos reales o simulados de niñas, niños o adolescentes en actitud sexual; será sancionada con pena privativa de libertad de trece a dieciséis años.

Si la víctima, además, sufre algún tipo de discapacidad o enfermedad grave o incurable, se sancionará con pena privativa de libertad de dieciséis a diecinueve años.

Cuando la persona infractora sea el padre, la madre, pariente hasta el cuarto grado de consanguinidad o segundo de afinidad, tutor, representante legal, curador o pertenezca al entorno íntimo de la familia; ministro de culto, profesor, maestro, o persona que por su profesión o actividad haya abusado de la víctima, será sancionada con pena privativa de libertad de veintidós a veintiséis años.”

- Los antecedentes negativos de Tik Tok: En julio de este año, la organización “Ecuador Dice No Más” publicó un comunicado señalando que Ecuador es uno de los principales productores de pornografía infantil en la región, y que existen medios cibernéticos que operan desde 6 ciudades, dedicadas a la propagación de tráfico, explotación sexual y trata de niños, niñas y adolescentes, “*crímenes que durante la pandemia se han incrementado mundialmente en un 40% debido al aislamiento*”.

7.2. Mobbing y Bullying

Son dos tipos de violencia que ya se hallan reconocidos por el Ecuador, tanto en el Código de Trabajo³³, como en la Ley Orgánica de Educación Intercultural³⁴, pero que al no encontrarse tipificados en nuestro COIP, se ha dificultado la sanción de estos ilícitos, dejando en vulnerabilidad o indefensión a muchas de las víctimas.

En tal virtud, se ha considerado oportuno y pertinente incluirlos como uno de los tipos de violencia que se tipifican con el presente proyecto de Ley, a efectos de no dejar por fuera ningún tipo de vulneración a los derechos de las y los ecuatorianos.

³³Código del Trabajo. “Art. (...).- (Agregado por el Art. 4 de la Ley s/n, R.O. 116-S, 9-XI-2017).- *Definición de acoso laboral: Debe entenderse por acoso laboral todo comportamiento atentatorio a la dignidad de la persona, ejercido de forma reiterada, y potencialmente lesivo, cometido en el lugar de trabajo o en cualquier momento en contra de una de las partes de la relación laboral o entre trabajadores, que tenga como resultado para la persona afectada su menoscabo, maltrato, humillación, o bien que amenace o perjudique su situación laboral. El acoso podrá considerarse como una actuación discriminatoria cuando sea motivado por una de las razones enumeradas en el artículo 11.2 de la Constitución de la República, incluyendo la filiación sindical y gremial.*

Las conductas que se denuncien como Acoso laboral serán valoradas por la autoridad de trabajo, según las circunstancias del caso, y la gravedad de las conductas denunciadas. La autoridad competente apreciará las circunstancias de acuerdo a la capacidad de estas de someter a un trabajador a presión para provocar su marginación, renuncia o abandono de su puesto de trabajo.”

³⁴ Ley Orgánica de Educación Intercultural. “Art. 64.2.- *Definición de acoso escolar.- (Agregado por el Art. 69 de la Ley s/n, R.O. 434-S, 19-IV-2021).- Se entiende por acoso escolar toda acción u omisión constitutiva de agresión u hostigamiento, directa o indirecta, repetitiva, realizada fuera o dentro del establecimiento educativo por estudiantes que, en forma individual o colectiva, atenten en contra de otro u otros, valiéndose para ello de una situación de superioridad o de indefensión del o los estudiantes afectados, que provoque maltrato, humillación, exclusión, burla o cualquier otra afectación a la dignidad, ya sea por medios tecnológicos o cualquier otro medio, tomando en cuenta su edad, identidad de género, identidad cultural, idioma, religión, ideología, condición socio-económica, condición migratoria, orientación sexual, estado de salud, discapacidad, diferencia física u otras de carácter temporal o permanente.”*

El acoso laboral consiste en un acto de violencia psicológica dirigida a producir miedo, terror, intimidación o perturbación mental en el trabajador, con la intención de provocar mengua en su capacidad física y psíquica, para por fin conseguir el abandono del trabajo.

La lengua inglesa utiliza el concepto de “*mobbing*” para referirse a la presión desmedida y la violencia simbólica que se ejerce dentro del entorno laboral. La persona que sufre este acoso puede ser atormentada con comentarios malintencionados o escuchar de manera recurrente críticas exageradas sobre su desempeño o su capacidad.³⁵

Marie France Hirigoyen, especialista en riesgos de trabajo define al acoso laboral como “*Toda conducta abusiva (gesto, palabra, comportamiento, actitud) que atenta por su repetición o sistematicidad contra la dignidad o la integridad psíquica o física de una persona, poniendo en peligro su empleo y degradando el ambiente de trabajo.*”³⁶

El acoso escolar o más conocido como *bullying* consiste en una persecución al menor que puede ser física o psicológica, con la intención de causar un mal al sujeto pasivo que sufre el acoso, situándolo en una posición de inferioridad respecto del agresores.³⁷

El *Bullying* comprende un catálogo de conductas, en general permanentes o continuadas en el tiempo y desarrolladas por uno o más alumnos sobre otro, susceptibles de provocar en la víctima sentimientos de terror, angustia e inferioridad, idóneos para humillarle, envilecerle y quebrantar, en su caso, su resistencia física y moral.³⁸

³⁵<https://dspace.unl.edu.ec/jspui/bitstream/123456789/8580/1/N%C3%A9stor%20Seraf%C3%ADn%20Gonz%C3%A1lez%20Gonz%C3%A1lez.pdf>

³⁶ HIRIGOYEN, Marie France, EL ACOSO LABORAL, Ed. Astrea, Bs. AS. Argentina, 2003, Pág. 15

³⁷ https://www.asociacionabogadosrcs.org/doctrina/doctrina_55_sandra_galvez.pdf

³⁸ (SAP de Madrid núm. 406/2014 de 9 de octubre)

Constituye, consecuentemente, el acoso escolar una modalidad de victimación que presenta como notas específicas las que a continuación se describen:³⁹

1. La existencia de conductas violentas de diversa naturaleza que tienen carácter persistente, prolongándose en el tiempo.
2. La confluencia de varios agresores que, bajo la dirección de uno o varios líderes, integran un grupo, intensificando con ello la sensación de dominio y favoreciendo distorsiones cognitivas en sus miembros (percepción absolutista, despersonalización, difuminación de la responsabilidad, culpabilización de la víctima).
3. La incardinación de una o varias víctimas con una estrategia de defensa limitada por la debilidad que caracteriza su posición, a quien se somete a dinámicas de exclusión y vejación.
4. La presencia del contexto educativo como vínculo o nexo entre los agresores y las víctimas. Se han destacado tres características de la escuela que contribuyen a la violencia escolar: la justificación o permisividad de la violencia como forma de resolución de conflictos entre iguales; el tratamiento habitual que se da a la diversidad actuando como si no existiera y la falta de respuesta del profesorado ante la violencia entre escolares.

7.3. Hostigamiento

El acoso y el hostigamiento sexual refieren conductas castigadas que violan la integridad y la libertad psicosexual de las personas.⁴⁰

Los comportamientos o conductas que puede llevar a cabo el agresor y que se constituyen como hostigamiento sexual son: los acercamientos innecesarios, abrazos o besos indeseados, familiaridad innecesaria, propuestas de contenido sexual, comentarios y preguntas sobre el aspecto, el estilo de vida, la orientación

³⁹ <http://biblio.upmx.mx/Estudios/Documentos/violenciabullying053.asp>

⁴⁰

https://www.researchgate.net/publication/315114077_Analisis_prevenion_y_atencion_del_hostigamiento_y_el_acoso_escolar_y_sexual_hacia_las_y_los_estudiantes_Caso_de_la_Universidad_Autonoma_del_Estado_de_Mexico

sexual, llamadas de teléfono ofensivas, comentarios o bromas sugestivas, reiteradas invitaciones a salir, gestos de connotación sexual, presentación de objetos pornográficos, miradas lujuriosas, fotos, afiches, protectores de pantalla, correos electrónicos, mensajes de texto sexualmente explícitos, uso de las diversas redes sociales electrónicas o digitales con fines sexuales. Sin embargo, la diferencia esencial con el acoso, radica en las maneras en que se llevan a cabo dichas propuestas, que en muchas ocasiones se realizan de manera velada, tal como lo señala la Organización Internacional del Trabajo (2014) en su Guía sobre Acoso sexual al referirse a las expresiones de chantaje sexual implícitas y explícitas.⁴¹

7.4. Molestias virtuales

Ciberacoso es acoso o intimidación por medio de las tecnologías digitales. Puede ocurrir en las redes sociales, las plataformas de mensajería, las plataformas de juegos y los teléfonos móviles. Es un comportamiento repetitivo que busca atemorizar, enfadar o humillar a otras personas. Los siguientes son claro ejemplos de acoso virtual.

- Difundir mentiras o publicar fotografías vergonzosas de alguien.
- Enviar mensajes hirientes o amenazas a través de plataformas informáticas.
- Hacerse pasar por otra persona y enviar mensajes agresivos en nombre de dicha persona⁴².

7.5. Ciberacoso sexual

Ciberacoso sexual, una forma de victimización en la que el agresor, adulto o menor, emplea técnicas agresivas, coercitivas y/o intimidatorias para conseguir lo que desea del menor⁴³. Cuando las técnicas empleadas no son agresivas, sino

⁴¹ https://www.redalyc.org/jatsRepo/884/88462046017/html/index.html#redalyc_88462046017_ref12

⁴² <https://www.unicef.org/es/end-violence/ciberacoso-que-es-y-como-detenerlo>

⁴³ https://www.researchgate.net/profile/Irene-Montiel/publication/275273999_Victimizacion_Infantil_Sexual_Online_Online_Grooming_Ciberabuso_

más bien lo contrario, de acercamiento amistoso o seductor y permiten el establecimiento de un vínculo emocional entre la víctima y su agresor, adulto, es más acertado hablar de Ciberabuso sexual, aunque muchos autores emplean los términos “*online grooming*”, “*child grooming*” o “*sexual grooming*”.

7.6. Exposición a contenidos nocivos

Se considera contenidos nocivos a todos aquellos mensajes que, aunque no inducen necesariamente al delito, resultan perjudiciales y hasta ofensivos para quienes los observan, especialmente para los menores ya que por su edad y madurez intelectual son más vulnerables ante contenidos que no pueden discernir con claridad (López J. D., 2014).⁴⁴

7.7. Trasmisión en vivo/*Streaming*

El *streaming* es un tipo de tecnología multimedia que envía contenidos de vídeo y audio a su dispositivo conectado a Internet. Esto le permite acceder a contenidos (TV, películas, música, pódcast) en cualquier momento que lo desee, en un PC o un móvil, sin someterse a los horarios del proveedor.⁴⁵

El *streaming* es lo que le permite consumir contenido en línea sin tener que esperar a que se descargue.

El *streaming* es un medio de enviar y recibir datos (como audio y vídeo) en un flujo continuo a través de una red. Esto permite que la reproducción comience mientras se envía el resto de los datos.⁴⁶

y_Ciberacoso_sexual/links/553692660cf268fd001870be/Victimizacion-Infantil-Sexual-Online-Online-Grooming-Ciberabuso-y-Ciberacoso-sexual.pdf

⁴⁴ López, J. D. (2014). La Protección De Los Menores De Edad En Internet: El Código Español Pasos En Materia De Alimentación Como Paradigma De Buenas Prácticas. Scielo, 2024-249.

⁴⁵ <https://www.avast.com/es-es/c-what-is-streaming>

⁴⁶ <https://www.avg.com/es/signal/what-is-streaming>

El *streaming* en vivo funciona de forma parecida al de otros tipos de contenido, pero se usa, sobre todo, para eventos especiales, como deportes o debates políticos.

Mientras se ve un *streaming* en vivo la transmisión se guarda temporalmente y se muestra en pequeñas cantidades de datos en su dispositivo, luego se descartan. Así, nunca recibirá el archivo; solo las partes que necesita en cada momento para su reproducción.

No todos los sitios de *streaming* son fiables. Si bien los grandes nombres, como *Netflix* y *Spotify* lo son, existen muchos sitios de *streaming* sospechosos.

7.8. Paliza feliz /Happy slapping

El término *happy slapping* (bofetada feliz, en español) nació en Reino Unido en 2005. El *happy slapping* consiste en la grabación de una agresión física, verbal o sexual y su difusión online mediante las tecnologías digitales (páginas, blogs, chats, redes sociales, etc.). Lo más común es que esta violencia se difunda por alguna red social y, en ocasiones, puede hacerse viral.⁴⁷

El *happy slapping* no siempre sigue una serie de normas, pero existen algunos patrones y fases comunes que podemos analizar para conocer más a fondo el fenómeno:

1. Acuerdo previo. Normalmente dos o más personas se ponen de acuerdo sobre cómo y cuándo poner en marcha una agresión física a otro compañero o compañera.
2. El pretexto. Los agresores suelen buscar una excusa para aislar a los niños o niñas que van a ser acosadas.

⁴⁷ <https://www.savethechildren.es/actualidad/happy-slapping-violencia-online-menores>

3. La agresión física. Cuando la víctima de *happy slapping* empieza a ser agredida suele haber una o más personas preparadas para grabar la escena y otros que golpean al menor.
4. Compartir las imágenes. Consiste en la difusión de esta violencia en canales digitales. Todo ello produce un daño constante a la víctima, que ve cómo se reproduce infinitamente su agresión.

La consecuencia que deja el *happy slapping* es que el daño que sufrió el menor quede persistente, pues de esta manera el menor agredido sufre humillaciones públicas continuadas. La visibilidad pública no solo hace que el daño a la víctima sea público, visible y viral, también puede dar lugar a nuevos ataques violentos.

7.9. Sextorsión / Chantaje Sexual

La Sextorsión supone el chantaje por parte de un ciberdelincuente para que la víctima realice una determinada acción o entregue una cantidad de dinero bajo la amenaza de publicar o compartid imágenes íntimas que de ella tiene. La casuística es muy variada siendo muy diversas las víctimas, las motivaciones y los daños finales que puedan llegar a provocarse.⁴⁸

En esta era digital conectada, dicha información podría incluir mensajes de texto sexuales, fotos íntimas e, incluso, vídeos. Los delincuentes suelen pedir dinero, pero a veces buscan material más comprometedor (envía más o divulgaremos tus secretos).⁴⁹

Según el Departamento de Justicia de los Estados Unidos, la "*sextorsión*" está catalogada como la amenaza cibernética más importante y de mayor crecimiento para los niños, con más víctimas menores por delincuente que todos los demás delitos de explotación sexual infantil.⁵⁰

⁴⁸ https://www.unodc.org/documents/ropan/2020/Ciberdelito_junio2020/SEXTORSION.pdf

⁴⁹ <https://www.kaspersky.es/blog/sextortion-stats/8863/>

⁵⁰ <https://www.intramed.net/contenidover.asp?contenidoid=93201>

7.10. Sexting no consentido / Violencia sexual digital

El término “*sexting*” es un neologismo que significa “*recibir, enviar o reenviar mensajes de texto, imágenes o fotografías que presentan un contenido sexual explícito, vía Internet o teléfono celular*”. La mayoría de estas imágenes, se diseminan de manera inmediata, incontrolada y extensa a través de las redes sociales, particularmente, los teléfonos celulares y computadoras, con resultados impredecibles, en la inmensa mayoría de las veces, catastróficos.

Investigaciones recientes indican que un número creciente de adolescentes ha enviado o “*posteados*” fotografías o videos de ellos mismos o de otros compañeros en situaciones comprometedoras (desnudos o semidesnudos, solos o acompañados, incluso en pleno escarceo erótico), ha representado graves problemas, incluyendo cargos criminales por felonía o pornografía, además de otras consecuencias, especialmente de orden emocional⁵¹.

7.11. Deep fake porn

Los *deepfakes* son videos o imágenes hiperrealistas manipulados digitalmente para representar a personas diciendo y haciendo cosas que en realidad nunca sucedieron. Los *deepfakes* se basan en redes neuronales que analizan grandes conjuntos de muestras de datos para aprender a imitar las expresiones faciales, los gestos, la voz y las inflexiones de una persona.⁵² El proceso implica introducir imágenes de dos personas en un algoritmo de aprendizaje profundo para entrenarlas para intercambiar caras. En otras palabras, los *deepfakes* usan tecnología de mapeo facial e inteligencia artificial que cambia la cara de una persona en un video por la cara de otra persona⁵³. Los *deepfakes* salieron a la luz en 2017 cuando un usuario de Reddit publicó videos que mostraban a

⁵¹ <http://www.scielo.org.mx/pdf/prh/v28n4/v28n4a7.pdf>

⁵² <https://link.springer.com/content/pdf/10.1007/s12119-020-09738-0.pdf>

⁵³ <file:///C:/Users/Hp/Downloads/66293-Texto%20del%20art%C3%ADculo-4564456576620-1-10-20191212.pdf>

celebridades en situaciones sexuales comprometedoras. Los *deepfakes* son difíciles de detectar, ya que utilizan metraje real, pueden tener audio con un sonido auténtico y están optimizados para difundirse rápidamente en las redes sociales. Por lo tanto, muchos espectadores asumen que el video que están viendo es genuino⁵⁴.

7.12. Creepshots

Una *creepshots* es, una foto tomada discretamente de mujeres en público por hombres está provocando preguntas sobre los derechos a la privacidad en público y preocupaciones éticas sobre la tecnología y la autonomía corporal⁵⁵.

Si bien las consecuencias negativas para las víctimas del acoso cibernético, *creepshots* y la pornografía de venganza a menudo son claras, tenemos dificultades para reconocer y abordar estos problemas porque nuestro marco culturalmente heredado para comprenderlos, e incluso nuestro lenguaje para describirlos, está codificado con suposiciones de que nuestras experiencias con o a través de tecnologías digitales están separadas y son distintas del resto de nuestras vidas.⁵⁶

7.13. Doxing

El *doxing* consiste en revelar información identificadora de una persona en línea, como su nombre real, dirección particular, lugar de trabajo, teléfono, datos financieros y otra información personal. Luego, esta información se divulga al público sin el permiso de la víctima.⁵⁷

Las motivaciones detrás del *doxing* varían. Puede que las personas sientan que fueron víctimas de ataques o insultos por parte de su objetivo y que, en respuesta, busquen venganza. Si alguien se hace famoso por sus opiniones

⁵⁴ <https://timreview.ca/article/1282>

⁵⁵ <https://spir.aoir.org/ojs/index.php/spir/article/view/8522/6791>

⁵⁶ <https://spir.aoir.org/ojs/index.php/spir/article/view/8522/6791>

⁵⁷ <https://latam.kaspersky.com/resource-center/definitions/what-is-doxing>

controversiales, podría atacar a alguien con puntos de vista opuestos. Sin embargo, este suele ser el caso cuando el tema tiene visiones especialmente polarizadas, en lugar de desacuerdos políticos cotidianos.

Estos son algunos de los métodos utilizados para atacar a las personas mediante el *doxing*:

- Rastrear los nombres de usuario.
- Ejecutar una búsqueda WHOIS en relación con un nombre de dominio.
- Suplantación de identidad (*phishing*).
- Seguimiento de las direcciones IP.
- Búsqueda inversa de teléfono celular.

Las situaciones más comunes de *doxing* por lo general se dividen en estas tres categorías:

- Divulgar en línea la información de identificación personal y privada de una persona.
- Revelar en línea información anteriormente desconocida de una persona privada.
- Divulgar en línea información de una persona privada podría ser perjudicial para su reputación y la de sus socios personales o profesionales.

7.14. *Outing*

El *outing* consiste en hacer público que una persona pertenece al colectivo LGTB sin su consentimiento. El *outing* es sacar del armario a una persona sin su consentimiento. En España decir que alguien es lesbiana, gay, trans*, bisexual o inter* no es delito si no hay dolor, o intención de vejar, despreciar o humillar.⁵⁸

⁵⁸ <https://linearcoiris.org/delito-odio/outing/>

7.15. Flaming

El *flaming* consiste en intimidar a las personas a través de Internet por medio de mensajes insultantes u hostiles.⁵⁹

Lo que hacen los que se denominan “*matones cibernéticos*”, en el caso del *flaming*, es generar polémica: empiezan temas de discusión que siembran tristeza, ira. Sentimientos que pueden ser encontrados, buscando el mínimo rescoldo para atacar a aquel que cuestiona su forma de pensar.

La principal razón de ser del *flaming* es que Internet garantiza el **anonimato**, y esto hace que cierto tipo de personas se aprovechen de él para emitir comentarios y opiniones que no se atreverían a dar si tuvieran que hacerlo a cara.⁶⁰

Un flame consiste en un mensaje deliberadamente hostil o insultante enviado sin ningún propósito constructivo; en consecuencia, *flaming* es el acto de publicar usualmente en el contexto social de un foro o una lista de correo electrónico, y aquel que los envía, recibe el nombre de *flamer*. A veces se publican como respuesta a un cebo, un mensaje provocativo, pensado especialmente para generar respuestas insultantes.

7.16. Sanciones propuestas en el COIP

TABLA No. 7
TIPOS DE VIOLENCIA DIGITAL - Sanciones propuestas

No.	TIPOS DE VIOLENCIA	ARTÍCULO COIP	SANCIÓN
1	Mobbing	Art. 154.2.- Acoso laboral.	• 1 a 3 años.
2	Bullying	Artículo 154.3.- Acoso escolar o académico.	• 1 a 3 años.
3	Hostigamiento	Art. 154.4.- Hostigamiento	• 6 meses a 1 año. En los siguientes casos:

⁵⁹ <http://ciberbullyngnea.blogspot.com/p/flaming.html>

⁶⁰ <https://rapinformes.es/sabes-que-es-el-flaming-por-internet/>

No.	TIPOS DE VIOLENCIA	ARTÍCULO COIP	SANCIÓN
			<ul style="list-style-type: none"> ✓ Buscar cercanía con la víctima. ✓ Establecer contacto con la víctima. ✓ Ofertar productos o servicios que no fueron solicitados por el sujeto pasivo. • 1 a 3 años (Si la víctima es mujer, menor de dieciocho años o discapacitada) • Máximo de pena. <ul style="list-style-type: none"> ✓ Intervengan miembros de la familia o afectivos. ✓ Cause afectación a la salud emocional.
4	Molestias virtuales	Art. 157.- Violencia psicológica contra la mujer o miembros del núcleo familiar. Segundo párrafo.	<ul style="list-style-type: none"> • 6 meses a 1 año. • 1 a 3 años. (Si se produce en la víctima, enfermedad o trastorno mental). • Máxima pena, aumentada en un tercio (Si la infracción recae en persona de uno de los grupos de atención prioritaria, en situación de doble vulnerabilidad o con enfermedades catastróficas o de alta complejidad).
5	Ciberacoso sexual	Art. 166.2. Acoso sexual. Segundo párrafo.	<ul style="list-style-type: none"> • 5 a 7 años (Uso de TICs para contacto con la víctima, con fines de naturaleza sexual). • 7 a 10 años (Si la víctima es mujer, menor de dieciocho años o discapacitada) • Máximo de pena. <ul style="list-style-type: none"> ✓ Intervengan miembros de la familia o afectivos. ✓ Cause afectación a la salud emocional. • Sanciones aumentadas en un tercio <ul style="list-style-type: none"> ✓ Causa daño personal, laboral, educativo, profesional o patrimonial. ✓ Sujeto activo fuera servidor público.
6	Exposición contenidos	Art. 169.- Corrupción de niñas, niños y adolescentes. Número 1.	<ul style="list-style-type: none"> • 3 a 5 años.

No.	TIPOS DE VIOLENCIA	ARTÍCULO COIP	SANCIÓN
	nocivos / Hipersexualización		
7	Trasmisión en vivo/Streaming	Art. 170.- Abuso sexual. Penúltimo párrafo. Art. 171. Violación. Número 6.	<ul style="list-style-type: none"> • 3 a 5 años. • 22 años (violación).
8	Happy slapping / Paliza feliz	Art. 170.- Abuso sexual. Último párrafo. Art. 171. Violación. Número 7.	<ul style="list-style-type: none"> • 3 a 5 años. • 22 años (violación).
9	Sextorsión / Chantaje sexual	Art. 172.1. – Extorsión sexual	<ul style="list-style-type: none"> • 5 a 7 años. • 7 a 10 años en los siguientes casos: <ul style="list-style-type: none"> ✓ Víctima grupo de atención prioritaria ✓ Relación laboral, de confianza o intervengan parientes (4° consanguinidad y 2° afinidad) ✓ Amenaza de muerte, lesión o secuestro ✓ Se comete desde un lugar de privación de libertad. ✓ Se comete desde el extranjero.
10	Sexting no consentido / Violencia Sexual Digital	Art. 178.- Violación a la intimidad. Párrafo quinto.	<ul style="list-style-type: none"> • 5 a 7 años (Contenido de carácter íntimo) • 7 a 10 años. En los siguientes casos: <ul style="list-style-type: none"> ✓ Si la víctima es mujer, menor de dieciocho años o discapacitada. ✓ Comercializar contenido sin consentimiento • Máximo de pena. <ul style="list-style-type: none"> ✓ Intervengan miembros de la familia o afectivos. ✓ Cause afectación a la salud emocional. • Cuando se cometa contra niñas, niños y adolescentes se sancionará conforme el Art. 103 y 104 del COIP.

No.	TIPOS DE VIOLENCIA	ARTÍCULO COIP	SANCIÓN
			<ul style="list-style-type: none"> • 3 meses a 1 año (Quienes contribuyan en el ilícito).
11	Deep fake porn	178.- Violación a la intimidad. Reales, simulados o alterados	<ul style="list-style-type: none"> • 3 a 5 años • 5 a 7 años (Contenido de carácter íntimo) • 7 a 10 años. En los siguientes casos: <ul style="list-style-type: none"> ✓ Si la víctima es mujer, menor de dieciocho años o discapacitada. ✓ Comercializar contenido sin consentimiento • Máximo de pena. <ul style="list-style-type: none"> ✓ Intervengan miembros de la familia o afectivos. ✓ Cause afectación a la salud emocional.
12	Creepshots	Art. 178.- Violación a la intimidad. Párrafo sexto.	<ul style="list-style-type: none"> • 7 a 10 años.
13	Doxing	Art. 179.- Revelación de secreto o información personal de terceros. Párrafo segundo.	<ul style="list-style-type: none"> • 1 a 3 años.
14	Outing	Art. 179.2. Revelación de secreto o información personal de terceros. Párrafo segundo.	<ul style="list-style-type: none"> • 1 a 3 años.
15	Flaming	Art. 396.1. - Contravenciones de cuarta clase.	<ul style="list-style-type: none"> • 15 a 30 días

8. DELITOS DE VIOLENCIA CONTRA LA MUJER O MIEMBROS DEL NÚCLEO FAMILIAR

Dentro de los tipos de violencia contra la mujer, que de igual forma se hallan ya reconocidos por el Ecuador, mediante la Ley Orgánica Integral para Prevenir y Erradicar la Violencia Contra las Mujeres, pero que asimismo, por no estar

tipificados en el COIP, muchas de las víctimas de estas inconductas han quedado en la indefensión a la espera de una justicia que casi no llega. A continuación desarrollamos brevemente cada uno de estos tipos de violencia para mayor ilustración y comprensión de la importancia de su tipificación.

8.1. Violencia económica y patrimonial

Hay quienes argumentan que la violencia económica (así como la simbólica, discutida más adelante) no deberían ser consideradas al mismo nivel que la violencia física y psicológica. Estos tipos generan el menor consenso intercultural como formas de "*violencia*". No obstante, los estudios muestran que el control coercitivo, una característica primordial de la violencia económica, se puede sentir incluso como algo peor que la violencia física para algunas mujeres. El control coercitivo incluye esfuerzos por "*herir, humillar, intimidar, explotar, aislar y dominar*" a las víctimas. Una estrategia fundamental de esta conducta es la negación o apropiación de recursos económicos (Stark, 2007, p. 5). Más aun, la violencia económica y simbólica raramente están aisladas, sino que forman parte de un patrón más amplio de agresiones que, en conjunto, tienen el efecto de crear un ambiente de trabajo hostil para las mujeres políticas.

La violencia económica raramente se menciona de manera explícita en la literatura sobre la violencia y el acoso político en América Latina (con la excepción de Medina Espino, 2013). Sin embargo, es posible encontrar ejemplos en las numerosas listas que se han generado, incluso es posible encontrar alusiones en la influyente legislación boliviana, bajo la categoría de "*violencia psicológica*". Este tipo de violencia puede iniciarse en el periodo de campaña. En México, por ejemplo, una reforma de 2008 buscaba estimular la participación política de las mujeres al requerir que los partidos políticos destinaran 2 por ciento de su financiamiento público para desarrollar actividades para promover el liderazgo femenino. Sin embargo, cuando las cuentas fueron revisadas en 2011 fue evidente que estos fondos se usaban para otros propósitos, como la compra de suministros de limpieza, papelería y servicios de fumigación (Romero, 2011). Incluso después de que Instituto Federal Electoral publicara una guía,

miembros de los partidos políticos le preguntaban abiertamente a los auditores cómo podían evitar destinar estos recursos para su propósito real. Mientras tanto, los grupos de mujeres al interior de los partidos políticos expresaban indignación y frustración dada la imposibilidad de acceder a estos fondos.

Problemas similares con fondos reservados para capacitación de las mujeres se han encontrado en Costa Rica, donde los partidos políticos han sido reacios a reportar cómo han gastado este dinero (Incer Brenes, 2014).

8.2. Violencia simbólica

La violencia simbólica opera al nivel de las representaciones y busca anular o borrar la presencia de las mujeres en las oficinas públicas. Estos comportamientos sólo han sido tangencialmente teorizados como "*violencia*" en los reportes de OSC sobre violencia contra mujeres en política. Sin embargo, estudios recientes sobre la misoginia y el sexismo en los medios de comunicación apoyan la conceptualización de ciertos comportamientos como formas de agresión, acoso y discriminación (Perks y Johnson, 2014; Sawer, 2013). Estas acciones no pueden verse como simples "*críticas constructivas*" o comportamientos groseros o irrespetuosos "*normales*" por parte de los medios, colegas u oponentes. El tratamiento negativo "*cruza la línea*" y se convierte en violencia cuando atenta contra la dignidad humana, como cuando se publican imágenes despectivas y altamente sexualizadas, se usan las redes sociales para promover la violencia, o no se reconoce a (o se niega abiertamente la existencia de) una mujer política simplemente por el hecho de ser mujer.

La "*violencia simbólica*" fue teorizada por Bourdieu (1984) como una manera de disciplinar a otros y confirmar el lugar en la jerarquía social de un individuo. Por lo tanto, la violencia simbólica puede ser mucho más poderosa que la violencia física puesto que está inmersa en la cultura, lo que hace que estas formas de violencia se sientan "*bien*" (Galtung, 1990). En consecuencia, las víctimas son con frecuencia "*cómplices*" de estos actos, y modifican sus comportamientos y aspiraciones de acuerdo con ellas, pero no los ven como herramientas de

dominación. Como Kraus (1993, p. 172) nota, la violencia simbólica puede ser muy efectiva para mantener la opresión de las mujeres porque es *"sutil, indirecta, invisible"*, tanto que incluso cuando algunas mujeres reconocen estos actos como ejercicios de poder, no les dan crédito, incluso en sociedades con altos niveles de equidad de género. Dada la gran diversidad de culturas en el mundo, la forma y el contenido de la violencia simbólica varían mucho más que los otros tres tipos, pero está presente en todas las sociedades.

8.3. Violencia política

La violencia contra las mujeres en política es parte de, pero es ligeramente diferente de, la violencia contra las mujeres en elecciones. Mientras que ésta incluye acciones dirigidas contra las mujeres candidatas, activistas y votantes durante el proceso electoral, la violencia contra las mujeres en política es cometida contra mujeres, tanto durante las campañas electorales como después, cuando las mujeres asumen posiciones políticas. Es vital reconocer que la crítica y el escrutinio de los candidatos y oficiales electos, así como de sus ideas y desempeño, es necesaria en todos los Estados. Más aún, la libertad de expresión es un elemento fundamental de una sociedad democrática sana. Sin embargo, ciertas conductas *"cruzan la raya"* cuando están dirigidas contra las mujeres por ser mujeres con el propósito de que se retiren de la contienda política. De esta manera, aunque son contra una mujer en particular, estas acciones están dirigidas, en efecto, contra todas las mujeres.

Cuando las mujeres políticas son atacadas solamente por sus ideas políticas no es un caso de violencia contra las mujeres en política. Sin embargo, la ambigüedad se hace evidente cuando la manera de atacarlas es a través del uso de estereotipos de género, enfocándose en sus cuerpos y los roles tradicionales, principalmente como madres y esposas, lo cual niega o socava su competencia en la esfera política. Usar imágenes o estereotipos de género para atacar a las oponentes mujeres, hace que las acciones se conviertan en un caso de violencia contra las mujeres en política, puesto que sugiere que las mujeres no pertenecen a lo político. Estas acciones tienen un profundo impacto puesto que no están

dirigidas contra una sola mujer sino que también tienen el propósito de intimidar a otras mujeres políticas, disuadir a otras mujeres que puedan considerar una carrera política y, peor aún, comunicar a la sociedad en general que las mujeres no deberían participar.

En este sentido, la violencia contra las mujeres en política tiene importantes similitudes con los delitos de odio, puesto que usa mecanismos de poder y opresión contra las personas con una identidad particular como una manera de reafirmar amenazas imaginadas contra las jerarquías tradicionales (Perry, 2001). Como los delitos de odio, la violencia contra las mujeres en política es un "*delito mensaje*", porque tiene como objetivo negar el acceso igualitario a los derechos, al tiempo que crea un efecto dominó que aumenta la sensación de vulnerabilidad entre otros miembros de ese grupo (Iganski, 2001). No obstante, en ambos casos hay dificultades puesto que no todas las víctimas experimentan la misma sensación de agravio. De hecho, algunas mujeres políticas pueden naturalizar estos comportamientos simplemente como el costo de estar en política, o pueden negar el problema, preocupadas por las acusaciones de ser "*histéricas*" o de no ser capaces de sobrellevar las demandas del trabajo, por miedo a justificar las acusaciones de que las mujeres no pertenecen a el ámbito político (Gillard, 2014).

8.4. Violencia mediática

La violencia mediática se refiere a la publicación o difusión de mensajes e imágenes estereotipados a través de cualquier medio masivo de comunicación, que de manera directa o indirecta promueva la explotación de mujeres o sus imágenes, injurie, difame, discrimine, deshonre, humille o atente contra la dignidad de las mujeres, como así también la utilización de ⁶¹mujeres, adolescentes y niñas en mensajes e imágenes pornográficas, legitimando la

⁶¹ https://www.argentina.gob.ar/sites/default/files/violenciasimbolica_recomendaciones.pdf

desigualdad de trato o construya patrones socioculturales reproductores de la desigualdad o generadores de violencia contra las mujeres.⁶²

Los efectos de la violencia mediática han sido encontrados en todos los tipos de medios examinados: TV, películas, videojuegos, música, dibujos animados, etc. (Anderson et al., 2003a; Kirsh, 2012). Los efectos son notablemente consistentes independientemente del tipo de medio, edad, sexo o lugar de residencia. Se puede concluir, por lo tanto, que, a pesar de la tendencia persistente, incluso entre algunas personas cultas, a negar los efectos de la violencia mediática (Anderson, Gentile y Dill, 2012), la investigación ofrece conclusiones bastante inequívocas (Media Violence Commission, 2012). Sorprendentemente, además, los avances se han producido en los planos más insospechados: los efectos de la violencia mediática usualmente toman formas menos dramáticas e instantáneas, es decir, no son inmediatos ni necesariamente severos. Por el contrario, se ha identificado un vínculo entre la exposición a la violencia mediática y la desensibilización, según se mide en la evaluación psicofisiológica y en la investigación conductual, tanto a corto como a largo plazo (Bailey, West y Anderson, 2011)⁶³.

8.5. Violencia gineco-obstétrica

Técnicamente *“La Gineco-obstetricia es la parte de la medicina que se ocupa de la reproducción humana y de las afecciones génito-mamarias. Por lo tanto, la temática está relacionada con el estudio anatómico, fisiológico y patológico del aparato génito-mamario, así como el embarazo, parto, puerperio normal y patológico”* (Salvatore, 2009, pp.1), a la vez, en la definición indicada en la Ley Orgánica Integral para Prevenir y Erradicar la Violencia de Género contra las Mujeres, también se contempla un abordaje social del concepto, relacionado también con el ejercicio de los derechos humanos.

⁶² <https://www.redalyc.org/pdf/105/10504704.pdf>

⁶³

http://www.injuve.es/sites/default/files/2018/47/publicaciones/1._influencia_en_la_violencia_de_los_medios_de_comunicacion._guia_de_buenas_practicas.pdf

“La violencia gineco-obstétrica, es una problemática social que todavía no está reconocida en la gran mayoría de países, y en nuestro país en particular no existen estadísticas ni estudios al respecto que permitan visualizar mejor su situación actual, según lo refiere el Informe Sombra al Comité de la Cedaw, que menciona por primera vez a este tipo de violencia en su artículo 12, concerniente a los derechos reproductivos de las mujeres” (Coque, 2016, p.7).

Como Coque indica se trata de una problemática social que ocurre a nivel mundial y que no es un hecho aislado, esto ha permitido que varios países pongan atención a esta práctica y la cuestionen.

Se trata de una violencia que no es tan fácil de reconocer y que a pesar de saber que se expresa en los procedimientos de interrupción de embarazos, en ninguna de las definiciones ubicadas, se encontró que no existe bibliografía que conceptualice esta relación y violencia gineco obstétrica.

En la violencia gineco obstétrica como en otras violencias se establecen relaciones de poder, existen dos referentes importantes Michael Foucault y Pierre Foucault, en el artículo de Hugo César Moreno, Licenciado Maestro en Sociología por la Universidad Iberoamericana titulado Bourdieu, Foucault y el poder, menciona:

Foucault define al poder como *“una relación de fuerzas, o más bien toda relación de fuerzas es una relación de poder [...] Toda fuerza ya es relación, es decir, poder: la fuerza no tiene otro objeto ni sujeto que la fuerza”*. Por el otro, Bourdieu profiere una tesis fundante, tesis eje del pensamiento bourdieano, donde el poder es presencia ineludible y éste aparece sólo como relación, como relación de fuerzas, enfrentamiento. Nos dice Bourdieu *“Todo poder de violencia simbólica, o sea, todo poder que logra imponer significados e imponerlas como legítimas disimulando las relaciones de fuerza en que se funda su propia fuerza, añade su fuerza propia, es decir, propiamente simbólica, a esas relaciones de fuerza”*. (Moreno, 2006, pp.2).

8.6. Sanciones propuestas en el COIP

TABLA No. 8
VIOLENCIA CONTRA LA MUJER – Sanciones propuestas

No.	TIPOS DE VIOLENCIA	ARTÍCULO COIP	SANCIÓN
1	Violencia económica y patrimonial	Art. 158.1. Violencia económica y patrimonial.	• 1 a 3 años
2	Violencia simbólica	Art. 158.2. Violencia simbólica.	• 1 a 3 años.
3	Violencia política	Art. 158.3. Violencia política.	• 1 a 3 años.
4	Violencia mediática	Art. 158.4. Violencia mediática	• 1 a 3 años.
5	Violencia gineco-obstétrica	Art. 158.5. Violencia gineco-obstétrica.	• 3 a 5 años.

9. DELITOS INFORMÁTICOS

9.1. Phishing

El origen de la palabra *Phishing* proviene del término *fishing* que significa pescar. Se identifica con esta palabra porque la intención de esta estafa es “*pescar*” a usuarios de internet para que releven información susceptible. Es decir, intentan que cojan el “*anzuelo*” y ofrezcan estos datos.

El *phishing* es una de las modalidades de estafa más utilizadas en la actualidad por los atacantes para intentar conseguir datos de gran importancia del usuario como su número de tarjeta de crédito, o cualquier información que después pueda ser utilizada de forma fraudulenta. El estafador, conocido habitualmente con el nombre de *phisher*, hace uso de técnicas de ingeniería social, haciéndose

pasar por una persona o empresa de total confianza y contactando mediante algún formato electrónico, generalmente un email idéntico al que suelen enviar esos contactos de confianza. Si la persona que recibe estos correos no tiene ciertos conocimientos, no será capaz de detectar que se trata de un fraude⁶⁴.

En estos mensajes se suele informar al usuario que tiene que entrar en una url para indicar de nuevo sus datos o algo similar, pero realmente, donde estamos entrando es a una dirección *web* totalmente falsa, en la que lo único que conseguiremos será proporcionar nuestra información al atacante.

Tradicionalmente el *phishing* está asociado al mundo del correo electrónico, pero además de esta vía, también se puede dar por otros medios como las redes sociales, llamadas telefónicas, el envío de SMS/MMS o incluso el uso del correo postal.⁶⁵

En los últimos años esta actividad ha ido mejorando y cada vez es más difícil detectar un correo falso. Además, las técnicas han ido mejorando considerablemente y cada día hay más y mejores. Actualmente se han contado más de 10.000 formas de phishing.

9.2. Pharming

En un concepto más amplio es una práctica fraudulenta semejante al *phishing*, con la diferencia de que en el primero, se manipula el tráfico legítimo de un sitio *web* para que dirija a los usuarios a sitios *web* falsos, pero muy similares en apariencia, que instalarán *software* malicioso en el equipo del visitante o que registrarán los datos personales del usuario, como sus contraseñas o sus datos bancarios.

⁶⁴ <https://www.acens.com/wp-content/images/2014/10/wp-phising-acens.pdf>

⁶⁵ 5 Anti-Phishing working group www.antiphishing.org

El *pharming* es especialmente peligroso porque, si afecta a un servidor DNS, incluso los usuarios con equipos protegidos y libres de malware pueden convertirse en víctimas. En un concepto más específico consiste también cuando el sujeto pasivo del delito clona una página institucional, por ejemplo, de una entidad financiera o de una compañía de comercio electrónico y el usuario de esta ingresa sus datos para realizar una transacción sin conocer que es falsa

9.3. Cloning o skimming

Se puede categorizar que es una forma común de clonar las tarjetas es mediante el uso de un *skimmer* de tarjetas. Se trata de un dispositivo de captura que permite a un delincuente registrar todos los datos en una tarjeta para poder sacar dinero de la cuenta de la víctima.

Un *skimmer* de tarjetas se coloca con mayor frecuencia en las ranuras para tarjetas de los cajeros automáticos, pero se sabe que los delincuentes los colocan en cualquier máquina que acepte tarjetas de débito y crédito.

Las desventajas menos sofisticadas de robar tarjetas también requieren que los delincuentes capturen su PIN por separado, por lo que instalarán una pequeña cámara apuntando al teclado. Estos suelen estar integrados en un frente falso de la máquina y pueden ser extremadamente difíciles de detectar. Muchas de las veces mediante este tipo penal se duplican o se clonan tarjetas, sin que tal hecho sea conocido por sus titulares, valiéndose de terceras personas como empleados de tiendas, a quienes los autores les proveen de artefactos electrónicos para copiar toda su información de la banda magnética.

9.4. Sanciones propuestas en el COIP

Tabla No. 9
DELITOS INFORMÁTICOS – Sanciones propuestas

No.	Delitos Informáticos	Artículos COIP	Sanción
1	Interceptación ilegal de datos	Art. 230.- Interceptación ilegal de datos	• 3 a 5 años
2	Phishing	Art. 230 número 1.- Interceptación ilegal de datos	• 3 a 5 años
3	Pharming	Art. 230 número 2.- Interceptación ilegal de datos	• 3 a 5 años
4	Cloning o skimming	Art. 230 número 4.- Interceptación ilegal de datos	• 3 a 5 años
5	Ataque a la integridad de sistemas informáticos	Art. 232.- Ataque a la integridad de sistemas informáticos	<ul style="list-style-type: none"> • 3 a 5 años • 5 a 7 años (Sobre bienes informáticos destinados a la prestación de un servicio público)
6	Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.	Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	• 3 a 5 años
7	Falsificación informática.	Artículo 234.1.- Falsificación informática	• 3 a 5 años

10. PROYECTO DE LEY ORGÁNICA REFORMATORIA DEL CÓDIGO ORGÁNICO INTEGRAL PENAL PARA PREVENIR Y COMBATIR LA VIOLENCIA SEXUAL DIGITAL Y FORTALECER LA LUCHA CONTRA LOS DELITOS INFORMÁTICOS

EXPOSICIÓN DE MOTIVOS

La violencia manifestada en las relaciones humanas como forma de control y poder con el fin de desvalorizar a otros y especialmente contra las mujeres, así como ser puerta para el abuso de niños, niñas y adolescentes, es una práctica que se encuentra naturalizada en las relaciones humanas y especialmente en las sociales, que no distingue edad, etnia, raza, condición económica, condición física, estado integral de salud, condición migratoria e identidad de sexo-genérica.

Es necesario reformar y actualizar la Ley Orgánica Integral para Prevenir y Erradicar la Violencia contra las Mujeres, así como el Código Orgánico Integral Penal para combatir las malas prácticas en el uso de las redes sociales que actualmente son herramientas que ampliaron las posibilidades de expresión y difusión de ideas y contenidos. Sin embargo, con ello también se acrecentó la vulnerabilidad y el peligro de todos los usuarios, ya sea por la difusión de información confidencial o por la comisión de diversos delitos que afecta la integridad de los estos.

Con profunda preocupación asistimos a la proliferación de conductas delictivas que vulneran el derecho a la privacidad de las personas y las exponen a situaciones de completa indefensión. Tales conductas tienen un efecto devastador sobre las mismas al lesionar gravemente su intimidad y su privacidad, todas estas conductas son violatorias del derecho a la privacidad de las personas.

La era de la conectividad en la que nos encontramos y cuyo antecedente exponencial se ubica en la última década del siglo pasado, viene vertiginosamente permeando todos los espacios de la vida. En algunos casos

aquel fenómeno ha permitido superar las limitaciones del del tiempo-espacio, pero a la vez ha generado fisuras que ponen en riesgo o relativizan la protección de algunos derechos fundamentales.

Los niveles de conectividad, la internet, las aplicaciones P2P, los teléfonos inteligentes, las redes sociales, diferentes aplicaciones; y, la virtualización en general ha provocado y en la mayoría de los casos han acentuado fenómenos anclados a la virtualización, entre ellos el *sexting* o el *stalking*.

El ciberacoso se define como la intimidación o agresión intencional y continua, a través de medios tecnológicos, electrónicos o digitales, como teléfonos móviles o internet que produce un desbalance entre acosado y acosador. Existen tres sujetos involucrados en este acto: el agresor, el agredido y el observador.

Por otro lado, uno de esos riesgos del *sexting* (Mensajes de textos de índole sexual) es la '*porno venganza*' y la '*extorsión sexual*', graves problemas que se han presentado en muchos países como Estados Unidos, México, Chile, Argentina, España, y demás países en el que el uso del internet no tiene restricciones, y entre esos nuestro país, donde hemos sido testigos de incontables casos de personas que han sido exhibidas y dañadas en su honor.

Insistimos en que las tecnologías de la Información y la Comunicación (TIC) nos han dado muchos beneficios y a la vez han abierto la oportunidad a ciertas personas en la sociedad para actuar fuera de la Ley al tratar de perjudicar a otros a través de lo que se conoce como acoso por medios tecnológicos, electrónicos o digitales, en el que se ataca a las víctimas de forma encubierta a través de las redes sociales o de las TIC's con el fin de infligir maltratos y denigraciones.

En Ecuador, según datos del INEC se estima que 15 934 522 personas es decir el 92% de la población mayor a 5 años cuenta con celulares y redes sociales, el 41,4% de la población cuenta con un teléfono inteligente de los cuales los picos más altos en la utilización, se encuentra entre en las edades comprendidas entre los 16 y 44 años de edad; y, de las cuales 6 240 889 personas utilizan redes sociales desde su *smartphone*. En el año 2018 según meta- análisis 1 de cada

7 adolescentes menores de 18 años había compartido material sensible y 1 de cada 4 lo había recibido. Es importante señalar, como dato adicional que, según estudios preliminares, la plataforma *WhatsApp* es la preferidas por comunidades digitales para compartir contenidos eróticos o sexuales mediante prácticas de *sexting* o *sexteo*.

Ante la problemática señalada, en Europa, Estados Unidos y Latinoamérica, ha crecido la necesidad de modificar las legislaciones actuales para incluir las normativas necesarias para evitar la difusión de videos, audios, fotografías reales o simulados a sabiendas que no existe consentimiento, sean estos impresos, mensajes de texto, correo electrónico, internet, redes sociales o cualquier otro medio, para evitar vulneraciones al derecho a la integridad y a la intimidad personal; y, también para reducir los ejercicios de coerción que el sujeto activo de la infracción ejerce mediante chantaje sobre el sujeto pasivo.

Los indicadores demuestran de manera alarmante que aproximadamente el 80% de las mujeres que viven algún tipo de violencia decide no tomar ninguna acción ante las autoridades y cuando lo hacen no continúan con la denuncia. Frente a esto, para proteger a la mujer, niñas, niños y adolescentes, personas con discapacidad y a toda la ciudadanía en general, de todo tipo de violencia en el entorno digital, es necesario manejar una legislación adecuada y mejorar la cooperación internacional, por lo que se plantea un marco regulatorio capaz de crear condiciones pertinentes para la adhesión no solo al Convenio de Budapest, sino a cualquier otro instrumento o convenio internacional en materia de combate a la violencia digital, a los delitos informáticos o ciberdelincuencia.

Los derechos de la mujer pueden ser regulados de manera adecuada, sancionando las formas de violencia contra el género o la mujer, que están consagradas en la Convención Interamericana de Belem Do Para y la Constitución de la República.

Con las nuevas tecnologías han surgido nuevos tipos de violencia y delitos en el entorno digital, que requieren ser regulados, sancionados y prevenidos de manera oportuna y efectiva, por lo que, es nuestro deber, legislar para la

protección de los ecuatorianos en todo tipo de espacios, adecuando las normas existentes para poder evolucionar casi a la misma velocidad que lo hace la sociedad, la tecnología o la *web*.

Lo virtual es real, es una dimensión parte de nuestra cotidianidad, que puede traer consecuencias irreparables en las víctimas de todo tipo de violencia en el entorno digital. Entre los daños ocasionados en las víctimas de violencia digital, que pueden ser varios, están: daño emocional, reputacional, físico y sexual, invasión de la privacidad, censura, suicidio y muerte. Actuar a tiempo ayuda a detectar y prevenir oportunamente la violencia sexual digital. Por ello, como Asamblea Nacional del Ecuador, hemos trabajado ineludiblemente y de la mano de quienes lamentablemente han sido víctimas y se han armado de valor para que todas y todos estemos seguros en la red.

REPÚBLICA DEL ECUADOR

ASAMBLEA NACIONAL

EL PLENO

CONSIDERANDO:

Que el artículo 1 de la Constitución de la República del Ecuador al establecer que el Ecuador es un Estado constitucional de derechos y justicia, social, democrático, soberano, independiente, unitario, intercultural, plurinacional y laico, enmarca al ordenamiento jurídico nacional dentro de los lineamientos de un Estado constitucional de derechos y justicia y, por consiguiente, es necesario realizar cambios normativos que respondan coherentemente al espíritu de la Constitución;

Que en el número 8 de artículo 11 de la Constitución de la República del Ecuador, se determina que el contenido de los derechos se desarrollará de manera progresiva a través de las normas, la jurisprudencia y las políticas

públicas. El Estado generará y garantizará las condiciones necesarias para su pleno reconocimiento y ejercicio;

Que en el número 3 literal a) del artículo 66 de la Constitución de la República del Ecuador se reconoce el derecho a la integridad personal que incluye, la integridad física, psíquica, moral y sexual;

Que en el número 3 literal b) del artículo 66 de la Constitución de la República del Ecuador se reconoce el derecho a la integridad personal que incluye, una vida libre de violencia en el ámbito público y privado; además de establecer que el Estado adoptará las medidas necesarias para prevenir, eliminar y sancionar toda forma de violencia, en especial la ejercida contra las mujeres, niñas, niños y adolescentes, personas adultas mayores, personas con discapacidad y contra toda persona en situación de desventaja o vulnerabilidad; idénticas medidas se tomarán contra la violencia, la esclavitud y la explotación sexual;

Que en el número 20 del artículo 66 de la Constitución de la República del Ecuador se reconoce el derecho a la intimidad personal y familiar;

Que la Constitución, de conformidad con el artículo 75, reconoce a las personas el derecho al acceso gratuito a la justicia y a la tutela efectiva, imparcial y expedita de sus derechos e intereses, con sujeción a los principios de inmediación y celeridad, y que en ningún caso quedarán en indefensión;

Que el número 3 del artículo 76 de la Constitución de la República del Ecuador, respecto a la garantía de estricta legalidad penal, establece que nadie podrá ser juzgado ni sancionado por un acto u omisión que, al momento de cometerse, no esté tipificado en la Ley como infracción penal, administrativa o de otra naturaleza; ni se le aplicará una sanción no prevista por la Constitución o la Ley. Sólo se podrá juzgar a una persona ante un juez o autoridad competente y con observancia del trámite propio de cada procedimiento;

Que de conformidad con el número 6 del artículo 76 de la Constitución se debe establecer la debida proporcionalidad entre las infracciones y las sanciones

penales, deben existir sanciones no privativas de la libertad, las que tienen que respetar los derechos de las personas y ser impuestas mediante procedimientos adversariales, transparentes y justos;

Que el artículo 78 de la Constitución prescribe que las víctimas de infracciones penales tendrán derecho a una protección especial, a no ser revictimizadas y a que se adopten mecanismos para una reparación integral que incluya el conocimiento de la verdad, restitución, indemnizaciones, rehabilitación, garantía de no repetición y satisfacción del derecho violado;

Que el artículo 82 de la Constitución de la República del Ecuador establece que el derecho a la seguridad jurídica se fundamenta en el respeto a la Constitución y en la existencia de normas jurídicas previas, claras, públicas y aplicadas por las autoridades competentes;

Que el artículo 84 de la Constitución de la República del Ecuador señala como garantía normativa que la Asamblea Nacional y todo órgano con potestad normativa tendrá la obligación de adecuar, formal y materialmente, las leyes y demás normas jurídicas a los derechos previstos en la Constitución y los tratados internacionales, y los que sean necesarios para garantizar la dignidad del ser humano o de las comunidades, pueblos y nacionalidades. En ningún caso, la reforma de la Constitución, las leyes, otras normas jurídicas ni los actos del poder público atentarán contra los derechos que reconoce la Constitución;

Que el número 6 del artículo 120 de la Constitución de la República del Ecuador establece como atribución y deber de la Asamblea Nacional, expedir, codificar, reformar y derogar las leyes, e interpretarlas con carácter generalmente obligatorio;

Que el número 2 del artículo 132 de la Constitución de la República establece que se requerirá de Ley en los siguientes casos: Tipificar infracciones y establecer las sanciones correspondientes;

Que el número 1 del artículo 134 de la Constitución de la República del Ecuador establece que la facultad de presentar proyectos de Ley le corresponde a las asambleístas y los asambleístas, con el apoyo de una bancada legislativa o de al menos el cinco por ciento de los miembros de la Asamblea Nacional;

Que en el inciso primero del artículo 424 de la Constitución, se establece que la Constitución es la Norma Suprema del Estado y prevalece sobre cualquier otra del ordenamiento jurídico y, por lo tanto, las normas y los actos del poder público deben mantener conformidad con las disposiciones constitucionales;

Que el sistema penal en su componente sustantivo mantiene tipos obsoletos, pues no responde a las necesidades actuales de la población; en su componente adjetivo es ineficiente y no ha logrado afianzar procesos justos, rápidos, sencillos, ni tampoco ha coordinado adecuadamente las acciones entre todos sus actores; y, en su componente ejecutivo no ha cumplido con sus objetivos y se ha convertido en un sistema poco eficaz, lo que justifica una reforma urgente al sistema penal en su conjunto; y,

En ejercicio de las atribuciones establecidas en el artículo 120 número 6 de la Constitución de la República y en el artículo 9 número 6 de la Ley Orgánica de la Función Legislativa, expide la siguiente:

LEY ORGÁNICA REFORMATORIA DEL CÓDIGO ORGÁNICO INTEGRAL PENAL PARA PREVENIR Y COMBATIR LA VIOLENCIA SEXUAL DIGITAL Y FORTALECER LA LUCHA CONTRA LOS DELITOS INFORMÁTICOS

Artículo 1.- Sustitúyase el primer párrafo del artículo 103 por el siguiente:

“Art. 103.- Pornografía con utilización de niñas, niños o adolescentes.- La persona que fotografíe, filme, grabe, produzca, transmita o edite materiales visuales, audiovisuales, informáticos, electrónicos o de cualquier otro soporte físico o formato que contenga la representación visual de desnudos o semidesnudos reales o simulados

de niñas, niños o adolescentes en actitud sexual, aunque el material tuviere su origen en el extranjero o fuere desconocido, será sancionada con pena privativa de libertad de trece a dieciséis años.

Artículo 2. – A continuación del artículo 154.1, agréguese los siguientes artículos:

“Art. 154.2. - Acoso laboral.- *Quien tenga un comportamiento atentatorio a la dignidad de la persona trabajadora, ejercido de forma reiterada, persistente, demostrable y potencialmente lesiva, cometido sobre un trabajador por parte de un empleador, jefe o superior jerárquico inmediato o mediato, o un compañero de trabajo o un subalterno, en el lugar de trabajo o fuera de él, ya sea por medio de cualquiera de las tecnologías de la información y comunicación o cualquier otro medio, que tenga como resultado para la persona afectada su menoscabo, maltrato, intimidación, terror, angustia, humillación, o bien que amenace o perjudique su situación laboral, genere desmotivación o induzca a la renuncia del mismo, será sancionada con pena privativa de libertad de uno a tres años.*

Art. 154.3.- Acoso escolar o académico.- *Se entiende por acoso escolar o académico a toda conducta negativa, intencional, metódica y sistemática de agresión, intimidación, ridiculización, difamación, coacción, aislamiento deliberado, amenaza, incitación a la violencia, hostigamiento o cualquier forma de maltrato psicológico, verbal, físico que, de forma directa o indirecta, dentro o fuera del establecimiento educativo, se dé por parte de un estudiante, docente, autoridad o con quienes mantiene una relación de poder asimétrica que, en forma individual o colectiva, atenten en contra de otro u otros, ya sea por medio de cualquiera de las tecnologías de la información y comunicación u otro medio, será sancionado con pena privativa de libertad de uno a tres años.*

Art. 154.4.- Hostigamiento. - *La persona natural o jurídica que, por sí misma o por terceros, moleste, perturbe o angustie de forma insistente o reiterada a otra, será sancionada con una pena privativa de la libertad de seis meses a un año, cuando concorra algunas de las siguientes circunstancias:*

- 1. El sujeto activo de la infracción busque cercanía con la víctima.*
- 2. El sujeto activo establezca o intente establecer contacto con la víctima a través de cualquier medio tecnológico, electrónico o digital, o por medio de terceras personas.*
- 3. El sujeto activo oferte productos o servicios que no fueron solicitados por el sujeto pasivo.*

Cuando la víctima sea mujer, o menor de dieciocho años de edad, o persona con discapacidad o cuando la persona no pueda comprender el significado del hecho o por cualquier causa no pueda resistirlo, será sancionada con pena privativa de libertad de uno a tres años.

Cuando este ilícito sea cometido por miembros del núcleo familiar o personas con las que se determine que el procesado o la procesada mantenga o haya mantenido vínculos familiares, íntimos, afectivos, conyugales, de noviazgo, de cohabitación, o de convivencia o aún sin ella, se aplicará el máximo de pena establecida en este artículo.

También se sancionará con el máximo de la pena establecida en este artículo, cuando producto de la afectación a la salud emocional de la víctima de este delito, se deriven o hayan derivado sobre sí misma conductas autolesivas, siempre que para la o el juzgador resulte demostrable que la afectación sufrida por la víctima fue determinante en el resultado dañoso autolesivo.”

Artículo 3.- Refórmese el artículo 157 por el siguiente:

“Art. 157.- Violencia psicológica contra la mujer o miembros del núcleo familiar. - Comete delito de violencia psicológica la persona que busca degradar o controlar acciones, comportamientos, pensamientos, creencias y decisiones, mediante amenaza, manipulación, chantaje, hostigamiento, humillación, o aislamiento, o cualquier otra conducta que cause afectación psicológica, contra la mujer o miembros del núcleo familiar, y será sancionada con pena privativa de libertad de seis meses a un año.

Será sancionada con la misma pena del inciso anterior, quien cometa este delito mediante la utilización de contenido íntimo o sexual, personal o de terceros, con el fin de provocar molestias virtuales que ocasionen afectación psicológica a la víctima.

Si con ocasión de la violencia psicológica se produce en la víctima, enfermedad o trastorno mental, la sanción será pena privativa de libertad de uno a tres años.

Si la infracción recae en persona de uno de los grupos de atención prioritaria, en situación de doble vulnerabilidad o con enfermedades catastróficas o de alta complejidad, la sanción será la máxima pena, aumentada en un tercio.”

Artículo 4.- A continuación del artículo 158, agréguese los siguientes artículos:

“Art. 158.1. Violencia económica y patrimonial. - Será sancionada con pena privativa de libertad de uno a tres años, toda acción u omisión que se dirija a ocasionar un menoscabo en los recursos económicos y patrimoniales de las mujeres, incluidos aquellos de la sociedad conyugal y de la sociedad de bienes de las uniones de hecho, a través de:

1. La perturbación de la posesión, tenencia o propiedad de sus bienes muebles o inmuebles;

2. *La pérdida, sustracción, destrucción, retención o apropiación indebida de objetos, instrumentos de trabajo, documentos personales, bienes, valores y derechos patrimoniales;*
3. *La limitación de los recursos económicos destinados a satisfacer sus necesidades o la privación de los medios indispensables para vivir una vida digna; así como la evasión del cumplimiento de sus obligaciones alimentarias;*
4. *La limitación o control de sus ingresos; y,*
5. *Percibir un salario menor por igual tarea, dentro de un mismo lugar de trabajo.*

Art. 158.2. Violencia simbólica. - *Será sancionada con pena privativa de libertad de uno a tres años, toda conducta que, a través de la producción o reproducción de mensajes, valores, símbolos, iconos, signos e imposiciones de género, sociales, económicas, políticas, culturales y de creencias religiosas, transmiten, reproducen y consolidan relaciones de dominación, exclusión, desigualdad y discriminación, naturalizando la subordinación de las mujeres.*

Art. 158.3. Violencia política. – *La persona o grupo de personas, que en contra de mujeres candidatas, militantes, electas, designadas o en funciones, defensoras de derechos humanos, feministas, lideresas políticas, sociales o comunitarias, o en contra de su familia, directa o indirectamente, menoscaben, anulen, obstaculicen, suspendan, impidan o restrinjan la participación política de la mujer, su accionar o el ejercicio de su cargo, o para inducirla u obligarla a que efectúe en contra de su voluntad una acción o incurra en una omisión, en el cumplimiento de sus funciones, incluida la falta de acceso a bienes públicos u otros recursos para el adecuado cumplimiento de sus funciones, será sancionada con pena privativa de libertad de uno a tres años.*

Art. 158.4. Violencia mediática. - *Aquella violencia cometida por una persona o grupo de personas a través de la publicación o difusión de información o contenido audiovisual o digital estereotipado, a través de cualquier medio de comunicación público, privado o comunitario que, de manera directa o indirecta, legitime la desigualdad de trato o construya patrones socioculturales reproductores o generadores de desigualdad, discriminación, cosificación, estigmatización o violencia contra las mujeres o en sus relaciones sociales, normalizando así, la subordinación de estas en la sociedad, será sancionada con pena privativa de libertad de uno a tres años.*

Art. 158.5. Violencia gineco-obstétrica. - *Toda acción, omisión, o patrón de conducta del personal de la salud, que limite el derecho de las mujeres embarazadas o no, a recibir servicios de salud gineco-obstétricos, expresada a través del maltrato, la imposición de creencias, prácticas culturales y científicas no consentidas, o la violación del secreto profesional, o la medicalización, y las no establecidas en protocolos, guías o normas, las acciones que consideren los procesos naturales de embarazo, parto y posparto como patologías, la esterilización forzada, la pérdida de autonomía y capacidad para decidir libremente sobre sus cuerpos y su sexualidad, impactando negativamente en la calidad de vida y salud sexual y reproductiva de las mujeres en toda su diversidad y a lo largo de su vida, cuando estas se realizan con prácticas invasivas, maltrato físico o psicológico, será sancionada con pena privativa de libertad de tres a cinco años.”*

Artículo 5.- Sustitúyase el artículo 166 por el siguiente:

“Art. 166.- Acoso sexual.- *La persona que solicite algún acto de naturaleza sexual, para sí o para un tercero, prevaleciendo de situación de autoridad laboral, docente, religiosa o similar, sea tutora o tutor, curadora o curador, ministros de culto, profesional de la educación o de la*

salud, personal responsable en la atención y cuidado del paciente o que mantenga vínculo familiar o cualquier otra forma que implique subordinación de la víctima, con la amenaza de causar a la víctima o a un tercero, un mal relacionado con las legítimas expectativas que pueda tener en el ámbito de dicha relación, será sancionada con pena privativa de libertad de tres a cinco años.

Se considerará ciberacoso sexual, cuando se utilice cualquiera de las tecnologías de la información y comunicación, medios tecnológicos, electrónicos o digitales, para establecer contacto con la víctima, con fines de naturaleza sexual, en beneficio propio o de terceros, que será sancionado con una pena privativa de libertad de cinco a siete años.

Cuando la víctima sea mujer, o menor de dieciocho años de edad, o persona con discapacidad o cuando la persona no pueda comprender el significado del hecho o por cualquier causa no pueda resistirlo, será sancionada con pena privativa de libertad de siete a diez años.

Cuando este ilícito sea cometido por miembros del núcleo familiar o personas con las que se determine que el procesado o la procesada mantenga o haya mantenido vínculos familiares, íntimos, afectivos, conyugales, de noviazgo, de cohabitación, o de convivencia o aún sin ella, se aplicará el máximo de pena establecida en este artículo, según el caso que corresponda.

También se sancionará con el máximo de la pena establecida en este artículo según el caso que corresponda, cuando producto de la afectación a la salud emocional de la víctima de este delito, se deriven o hayan derivado sobre sí misma conductas autolesivas, siempre que para la o el juzgador resulte demostrable que la afectación sufrida por la víctima fue determinante en el resultado dañoso autolesivo.

En todo momento el juzgador debe garantizar que ninguna actuación o diligencia implique una revictimización a la persona agredida, para lo cual,

deberá contemplar métodos alternativos que le permitan avanzar sin dilaciones con la investigación.

Los hechos descritos en este artículo serán perseguibles mediante denuncia de la persona agraviada o por cualquier otra persona o entidad que tuviere conocimiento del presunto cometimiento de este ilícito. Una vez iniciada la investigación, la autoridad competente impulsará la causa de oficio hasta obtener una resolución judicial ejecutoriada en que se pronuncie sobre este ilícito.

La persona que solicite favores de naturaleza sexual que atenten contra la integridad sexual de otra persona, y que no se encuentre previsto en el inciso primero de este artículo, será sancionada con pena privativa de libertad de seis meses a dos años.

Las sanciones aumentarán en un tercio en los siguientes casos:

- a. Si el sujeto activo causa un daño personal, laboral, educativo, profesional o patrimonial; o,*
- b. Si el sujeto activo fuere servidor público y utilizare los medios propios del cargo, además de la destitución e inhabilitación para ocupar empleo o cargo público, por un período igual al de la pena privativa de libertad impuesta.”*

Artículo 6.- Sustitúyese el artículo 169 por el siguiente:

“Art. 169.- Corrupción de niñas, niños y adolescentes. -

- 1. La persona que permita el acceso o exposición de niñas, niños o adolescentes de forma intencionada a contenido nocivo sexualizado, violento, o generador de odio, será sancionada con pena privativa de libertad de uno a tres años.*
- 2. La persona que incite, conduzca o permita la entrada de niñas, niños o adolescentes a prostíbulos o lugares en los que se exhibe*

pornografía, será sancionada con pena privativa de libertad de tres a cinco años.”

Artículo 7.- Al final del artículo 170, inclúyase lo siguiente:

“Se sancionará con el máximo de la pena establecida en este artículo, cuando dicho abuso sexual fuese grabado o transmitido en vivo de manera intencional por la persona agresora, por cualquier medio digital, dispositivo electrónico o a través de cualquiera de las tecnologías de la información y comunicación.

Asimismo, se sancionará con el máximo de la pena establecida en este artículo, cuando además de la grabación o transmisión de este abuso sexual con cualquier medio digital, dispositivo electrónico o a través de cualquiera de las tecnologías de la información y comunicación, se agrede físicamente a la víctima, y dicha agresión también sea grabada o transmitida.”

Artículo 8.- A continuación del número 5 del artículo 171, inclúyanse los siguientes números:

“6. Cuando dicha violación fuese grabada o transmitida en vivo de manera intencional por la persona agresora, por cualquier medio digital, dispositivo electrónico o a través de cualquiera de las tecnologías de la información y comunicación.

7. Cuando además de la grabación o transmisión de esta violación con cualquier medio digital, dispositivo electrónico o a través de cualquiera de las tecnologías de la información y comunicación, se agrede físicamente a la víctima, y dicha agresión también sea grabada o transmitida.”

Artículo 9.- Luego del artículo 172, agréguese el siguiente artículo:

“Art. 172.1. – Extorsión sexual. - La persona que, mediante el uso de violencia, amenazas, manipulación o chantaje, induzca, incite u obligue a otra a exhibir su cuerpo desnudo, semidesnudo, o en actitudes sexuales, con el propósito de obtener un provecho personal o para un tercero, ya sea de carácter sexual o de cualquier otro tipo, será sancionada con pena privativa de libertad de cinco a siete años.

La sanción será de siete a diez años si se verifican alguna de las siguientes circunstancias:

1. *Si la víctima es una persona menor a dieciocho años, mayor a sesenta y cinco años, mujer, o persona con discapacidad, o una persona que padezca enfermedades que comprometan su vida.*
2. *Si se ejecuta con la intervención de una persona con quien la víctima mantenga relación laboral, comercio u otra similar o con una persona de confianza o pariente dentro del cuarto grado de consanguinidad y segundo de afinidad.*
3. *Si el constreñimiento se ejecuta con amenaza de muerte, lesión, secuestro o acto del cual pueda derivarse calamidad, infortunio o peligro común.*
4. *Si se comete total o parcialmente desde un lugar de privación de libertad.*
5. *Si se comete total o parcialmente desde el extranjero.”*

Artículo 10.- Al final del número 2 del artículo 175, agréguese lo siguiente:

“Una vez emitidas las medidas cautelares, el Juez de Garantías Penales también podrá ordenar se dispongan las medidas de protección necesarias, a las Juntas Cantonales y Metropolitanas de Protección de Derechos o a las o los Jueces de Familia, Mujer, Niñez y Adolescencia, o multicompetentes, con el fin de que se realice un abordaje integral para la

protección y restitución de derechos de mujeres; niñas, niños o adolescentes; o, personas con discapacidad.”

Artículo 11.- Sustitúyase el artículo 178, por el siguiente:

“Art. 178.- Violación a la intimidad. - *La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, grabe, revele, difunda, publique o dé algún tratamiento indebido o no autorizado a contenido de terceros, datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, contenidos digitales o comunicaciones privadas o reservadas, por cualquier medio o por intermedio de cualquiera de las tecnologías de la información y comunicación, será sancionada con pena privativa de libertad de uno a tres años.*

Se sancionará con la misma pena del primer párrafo, cuando:

- a. El contenido divulgado sea extraído de cualquier dispositivo electrónico que no sea de propiedad del infractor, ya sea que este lo haya robado, hurtado o encontrado; o, este haya sido previamente extraviado por su legítimo propietario, lo que será debidamente comprobado por la autoridad competente.*
- b. El contenido divulgado sea extraído de alguna plataforma digital a la cual el infractor tenga acceso, ya sea a gratuita o pagada; y extraiga sin consentimiento contenido de terceros, de carácter personal o íntimo, que contenga la representación visual de desnudos, semidesnudos, o actitudes sexuales.*

Se considerará como violencia sexual digital, cuando se trate de contenido de terceros, de carácter personal o íntimo, que contenga la representación visual de desnudos, semidesnudos, o actitudes sexuales que la persona afectada le hubiese confiado de su intimidad, reales, simuladas o alteradas, que será sancionada con una pena privativa de libertad de cinco a siete años.

Cuando dicho contenido hubiese sido obtenido de manera clandestina o sin que el sujeto se dé cuenta, se impondrá una pena privativa de libertad de siete a diez años.

Cuando la víctima sea mujer, o persona con discapacidad o cuando la persona no pueda comprender el significado del hecho o por cualquier causa no pueda resistirlo, será sancionada con pena privativa de libertad de siete a diez años.

Asimismo, será sancionado con la misma pena del párrafo anterior, quien comercialice por correo electrónico, chat, mensajería instantánea, redes sociales, blogs, foto blogs, juegos en red o cualquier otro medio electrónico o telemático a través de cualquiera de las tecnologías de la información y comunicación, fotos, videos, sin consentimiento de la persona que aparece en estos medios.

Cuando se cometa contra niñas, niños o adolescentes, se estará acorde a lo establecido en los artículos 103 y 104 de este Código, según corresponda.

Cuando este ilícito sea cometido por miembros del núcleo familiar o personas con las que se determine que el procesado o la procesada mantenga o haya mantenido vínculos familiares, íntimos, afectivos, conyugales, de noviazgo, de cohabitación, o de convivencia o aún sin ella, se aplicará el máximo de pena establecida en este artículo, según el caso que corresponda.

Cuando producto de la afectación a la salud emocional de la víctima de este delito, se deriven o hayan derivado sobre sí misma conductas autolesivas, siempre que para la o el juzgador resulte demostrable que la afectación sufrida por la víctima fue determinante en el resultado dañoso autolesivo, se sancionará al infractor con el máximo de la pena establecida en este artículo, según el caso que corresponda.

Una vez iniciadas las investigaciones, la autoridad competente deberá mantener el contenido digital en reserva y bajo la debida custodia; y, únicamente podrá ser dado de baja en el momento procesal oportuno, a petición de parte y previa autorización judicial. Se precautelaré que antes de eliminar o bajar dicho contenido, se deje el rastro o resguardo suficiente para que no se pierda la cadena de custodia de elementos que pueden ser sustanciales en la investigación.

En todo momento el juzgador debe garantizar que ninguna actuación o diligencia implique una revictimización a la persona agredida, para lo cual, deberá contemplar métodos alternativos que le permitan avanzar con la investigación.

Los hechos descritos en este artículo serán perseguibles mediante denuncia de la persona agraviada o por cualquier otra persona o entidad que tuviere conocimiento del presunto cometimiento de este ilícito. Una vez iniciada la investigación, la autoridad competente impulsará la causa de oficio hasta obtener una resolución judicial ejecutoriada en que se pronuncie sobre este ilícito.

Todos quienes participen o contribuyan en el cometimiento de este ilícito, serán sancionados con una pena privativa de libertad de tres meses a un año. Esta participación deberá ser debidamente comprobada y determinada como tal por la o el juzgador.

No son aplicables estas normas para la persona que divulgue información pública de acuerdo con lo previsto en la Ley.”

Artículo 12.- A continuación del artículo 178, agréguese el siguiente artículo:

“Art. 178.1.- Disposiciones especiales del delito de violación a la intimidad. - Para el delito de violación a la intimidad, se observarán las siguientes disposiciones especiales:

1. *En este delito, la o el juzgador, adicional a la pena privativa de libertad puede imponer una o varias penas no privativas de libertad.*
2. *En los casos en los que la o el presunto agresor sea ascendiente o descendiente o colateral hasta el cuarto grado de consanguinidad o segundo de afinidad, cónyuge, excónyuge, conviviente, ex conviviente, pareja o ex pareja en unión de hecho, tutora o tutor, representante legal, curadora o curador o cualquier persona a cargo del cuidado o custodia de la víctima, el Juez de Garantías Penales como medida cautelar suspenderá la patria potestad, tutoría, curatela y cualquier otra modalidad de cuidado sobre la víctima a fin de proteger sus derechos. Esta medida también la podrá solicitar la o el fiscal, de oficio o petición de parte la o el juez competente. Una vez emitidas las medidas cautelares, el Juez de Garantías Penales también podrá ordenar se dispongan las medidas de protección necesarias, a las Juntas Cantonales y Metropolitanas de Protección de Derechos o a las o los Jueces de Familia, Mujer, Niñez y Adolescencia, o multicompetentes, con el fin de que se realice un abordaje integral para la protección y restitución de derechos de mujeres; niñas, niños o adolescentes; o, personas con discapacidad.*
3. *Para este delito no será aplicable la atenuante prevista en el número 2 del artículo 45 de este Código.*
4. *El comportamiento público o privado de la víctima, anterior a la comisión de la infracción, no es considerado dentro del proceso.*
5. *En este delito el consentimiento dado por la víctima menor de dieciocho años de edad es irrelevante.*
6. *Las víctimas en este delito pueden ingresar al programa de víctimas y testigos.”*

Artículo 13.- Sustitúyase el artículo 179 por el siguiente:

“Art. 179.- Revelación de secreto o información personal de terceros.

- La persona que teniendo conocimiento de un secreto o información personal de terceros cuya divulgación pueda causar daño a otra persona y lo revele, será sancionada con pena privativa de libertad de seis meses a un año.

Quien revele o divulgue contenido digital, mensajes, correos, imágenes, audios o videos o cualquier otro contenido personal o datos íntimos sobre la sexualidad de una persona sin su consentimiento, en virtud de que ha querido mantener esta información en secreto, será sancionada con pena privativa de libertad de uno a tres años.”

Artículo 14. - Sustitúyase el artículo 230, por el siguiente:

“Art. 230.- Interceptación ilegal de datos. - *Será sancionada con pena privativa de libertad de tres a cinco años:*

- 1. La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma, contenido digital en su origen, destino o en el interior de un sistema informático o dispositivo electrónico, una señal o una transmisión de datos o señales.*
- 2. La persona que ilegítimamente diseñe, desarrolle, ejecute, produzca, programe o envíe contenido digital, códigos de accesos o contraseñas, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.*
- 3. La persona que posea, venda, distribuya o, de cualquier otra forma, disemine o introduzca en uno o más sistemas informáticos,*

dispositivos electrónicos, programas u otros contenidos digitales destinados a causar lo descrito en el número anterior.

- 4. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.*
- 5. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos, o programas o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior.”*

Artículo 15. – Sustitúyase el artículo 232, por el siguiente:

“Art. 232.- Ataque a la integridad de sistemas informáticos. - *La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento o comportamiento no deseado, o suprima total o parcialmente contenido digital, sistemas informáticos, sistemas de tecnologías de la información y comunicación, dispositivos electrónicos o infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general, con el propósito de obstaculizar de forma grave, deliberada e ilegítima el funcionamiento de un sistema informático, será sancionada con pena privativa de libertad de tres a cinco años.*

Con igual pena será sancionada la persona que diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos, programas o sistemas informáticos maliciosos o destinados a causar los efectos señalados en el primer inciso de este artículo.

Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad.”

Artículo 16. – Sustitúyase el artículo 234, por el siguiente:

“Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.

1. La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, será sancionada con la pena privativa de la libertad de tres a cinco años.

2. Si la persona que accede al sistema lo hace para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o re direccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad cinco a siete años.”

Artículo 17. – A continuación del artículo 234, agréguese los siguientes artículos:

“Art. 234. 1. - Falsificación informática:

1. La persona que, con intención de provocar un engaño en las relaciones jurídicas, introducir, modificar, eliminar o suprimir contenido digital, o interferir de cualquier otra forma en el tratamiento informático de datos, produciendo datos o documentos no genuinos, será sancionada con pena privativa de libertad de tres a cinco años.

2. Quien, actuando con intención de causar un perjuicio a otro o de obtener un beneficio ilegítimo para sí o para un tercero, use un documento producido a partir de contenido digital que fuera objeto de los actos referidos en el número 1, será sancionado con la misma pena.”

“Art. 234. 2. - Agravación de las penas. - La práctica de los hechos que se describen en los artículos 232, 234 y 234.1 será sancionada con pena agravada en un tercio de su pena máxima si logra perturbar de forma grave o duradera a un sistema informático que apoye una actividad destinada a asegurar funciones sociales críticas, como cadenas de abastecimiento, salud, seguridad y bienestar económico de las personas, o funcionamiento regular de los servicios públicos.”

“Art. 234. 3. - Responsabilidad de personas jurídicas. - A los delitos de esta Sección es aplicable la responsabilidad prevista en el artículo 49 y 71 de este Código.”

“Art. 234.4. – Definiciones. - Para los efectos del presente Código, se considera:

- a. **Contenido digital.** - El contenido digital es todo dato informático que representa hechos, información o conceptos de la realidad, almacenados, procesados o transmitidos por cualquier medio tecnológico o canal de comunicación que se preste a tratamiento informático, incluidos los programas diseñados para un equipo tecnológico aislado, interconectado o relacionados entre sí.
- b. **Datos de tráfico.** - Contenido digital relativo a una comunicación efectuada por medio de un sistema informático o canal de comunicación, generados por este sistema como elemento de una cadena de comunicación, indicando su origen, su destino, su trayecto, la hora, la fecha, el tamaño, la duración o el tipo de servicio subyacente.
- c. **Proveedor de servicios.** - Cualquier entidad, pública o privada, nacional o internacional, que proporciona a los usuarios de sus servicios la capacidad de comunicarse a través de un sistema

informático, o de cualquiera de las tecnologías de la información y comunicación, así como cualquier otra entidad que procese o almacene contenido digital en nombre y por cuenta de aquella entidad proveedora o de sus usuarios.

- d. **Sistema informático.** - *Cualquier dispositivo o conjunto de dispositivos interconectados o asociados, en que uno o varios de ellos desarrolla, ejecutando un programa, el tratamiento automatizado de contenido digital.”*

Artículo 18. – Reemplácese el número 1 del artículo 396, por el siguiente:

“1. La persona que, por cualquier medio, inclusive a través de cualquiera de las tecnologías de la información y comunicación, profiera expresiones en descrédito o deshonra en contra de otra, ya sea mediante lenguaje violento, agresivo, vulgar u hostil.”

Artículo 19. - A continuación del artículo 477, agréguese el siguiente artículo:

“Art. 477. 1. - Interceptación de las comunicaciones en cooperación internacional. - *En ejecución de una petición de una autoridad extranjera competente, puede ser ordenada la interceptación de transmisiones de contenido digital realizadas por medio de un sistema informático ubicado en el Ecuador, si así se prevé en algún acuerdo, tratado o convenio internacional vigente previamente reconocido por el Ecuador, que haya pasado en legal y debida forma por el respectivo control previo de constitucionalidad, y si se trata de situación en la que dicha interceptación está permitida en un caso nacional de características similares, respetándose el procedimiento y observándose los límites y garantías previstos en el derecho interno.”*

Artículo 20.- Después del artículo 497, incorpórese la siguiente sección:

“SECCIÓN CUARTA

Obtención de Prueba por Medio de Cooperación Internacional

Art. 497. 1. - Cooperación internacional. - *Las autoridades nacionales competentes cooperarán con las autoridades extranjeras competentes que así lo soliciten, en las investigaciones o procedimientos que sean necesarios para la obtención de indicios o pruebas en formato digital, relativos a delitos relacionados con las tecnologías de la información y comunicación, o; con sistemas informáticos o contenido digital.*

Art. 497. 2. - Preservación y divulgación expedita de contenido digital en la cooperación internacional.

1. *Se puede solicitar al Ecuador la preservación expedita de contenido digital almacenado en un sistema informático aquí ubicado, con el objetivo de presentar una solicitud de asistencia para la búsqueda, incautación y divulgación de los mismos.*
2. *La solicitud especificará:*
 - a. *La autoridad que solicita la preservación;*
 - b. *El delito que está siendo investigado, así como un breve resumen de los hechos conexos;*
 - c. *El contenido digital que debe conservarse y su relación con el delito;*
 - d. *Toda la información disponible para identificar a la persona responsable del contenido digital o la ubicación del sistema informático;*
 - e. *La necesidad de la preservación, y,*
 - f. *La intención de presentar una solicitud de ayuda para la búsqueda, incautación y difusión de datos.*
3. *En la ejecución de una solicitud de autoridad extranjera competente en virtud de los números anteriores, la o el juzgador, dará la orden a quién tenga el control o disponibilidad de estos datos, incluido el proveedor de servicios, para que este los preserve.*
4. *La orden de preservación especificará, bajo pena de nulidad:*

- a. *La naturaleza de los datos;*
 - b. *Si se conocen, su origen y su destino, y,*
 - c. *El período de tiempo durante el cual los datos deben conservarse hasta un máximo de tres meses.*
5. *En cumplimiento de la orden de preservación dirigida hacia él, quien tenga el control o la disponibilidad de estos datos, incluyendo el proveedor de servicios, preservará de inmediato los datos en cuestión por el período especificado, protegiendo y conservando su integridad.*
 6. *La o el juzgador, podrá ordenar la renovación de la medida por períodos sujetos al límite previsto en el literal c) del número 5, siempre que se verifiquen sus requisitos de admisibilidad, hasta un máximo un año.*
 7. *Cuando sea presentada la solicitud de ayuda contemplada en el número 1, la o el juzgador, determinará la preservación de los datos hasta la adopción de una decisión definitiva sobre la solicitud.*
 8. *Los datos preservados en virtud del presente artículo se concederán únicamente a:*
 - a. *Al solicitante de la ayuda contemplada en el número 1, de la misma manera que podría hacerse en un caso nacional de características similares;*
 - b. *A la autoridad nacional que emitió la orden de preservación, en las mismas condiciones que podrían realizarse en un caso similar nacional.*
 9. *Las disposiciones de los apartados 1 y 2, se aplicarán, con las debidas adaptaciones, a las peticiones formuladas por las autoridades del Ecuador a autoridades extranjeras.*

Art. 497. 3. - Motivos de denegación.

1. *La solicitud de preservación o divulgación expedita de contenido digital será denegada cuando:*

- a. *El contenido digital en cuestión se refiera a un delito político o delito conexo de acuerdo con los conceptos del derecho del Ecuador; y,*
 - b. *Atenten contra la soberanía, seguridad, orden público u otros intereses del Ecuador.*
2. *La solicitud de preservación expedita de contenido digital podrá aún ser denegada si existieren motivos razonables para creer que la ejecución de la subsecuente solicitud de ayuda para fines de búsqueda, incautación y divulgación de tales datos será rechazada por falta de comprobación del requisito de la doble incriminación.*

Art. 497. 4. - Acceso a contenido digital en la cooperación internacional.

1. *En ejecución de una solicitud de autoridad extranjera competente, y de acuerdo con las normas de derecho nacional, se procederá al registro e incautación y la divulgación de datos almacenados en un sistema informático ubicado en el Ecuador, cuando se trate de una situación en que el registro e incautación son admisibles en un caso nacional de características similares.*
2. *Las autoridades nacionales actuarán, en el ámbito de sus competencias, tan pronto como sea posible, cuando existieran razones para creer que el contenido digital en cuestión es especialmente vulnerable a su pérdida o modificación, o cuando la cooperación rápida esté prevista en un instrumento internacional aplicable.*
3. *Las disposiciones del número 1 se aplicarán, con las debidas adaptaciones, a las peticiones formuladas por las autoridades del Ecuador a autoridades extranjeras.*

Art. 497. 5. - Acceso transfronterizo a contenido digital almacenado de acceso público o con consentimiento.

1. *Las autoridades extranjeras competentes, podrán:*
 - a. *Acceder a contenido digital almacenado en un sistema informático ubicado en el Ecuador, cuando éste esté a disposición del público;*
 - b. *Recibir o acceder, por medio de un sistema informático ubicado en su territorio, a contenido digital almacenado en el Ecuador, con el consentimiento legal y voluntario de la persona legalmente autorizada a revelarlos.*

2. *Las mismas facultades tendrán las autoridades del Ecuador, con relación a contenido digital alojado en el extranjero.*

Art. 497. 6. - Punto permanente de contacto para la cooperación internacional.

1. *A los fines de la cooperación internacional, tanto la Policía Nacional, como la Fiscalía General del Estado y el Consejo de la Judicatura, mantendrán una estructura que garantice un punto de contacto disponible en todo momento, las veinticuatro horas del día, los siete días de la semana.*
2. *Esta estructura podrá ser contactada por sus pares extranjeros, con arreglo a los acuerdos, tratados o convenios internacionales vigentes previamente reconocidos por el Ecuador, que hayan pasado en legal y debida forma por el respectivo control previo de constitucionalidad, o en ejecución de protocolos de cooperación internacional con organismos judiciales o policiales.*
3. *La asistencia inmediata que ofrece este punto de contacto permanente incluye:*
 - a. *La prestación de asesoramiento técnico a otros puntos de contacto;*
 - b. *La preservación expedita de datos en casos de urgencia o peligro en el retraso, en conformidad con el artículo siguiente;*

- c. *La recopilación de pruebas para las que tiene jurisdicción en casos de urgencia o de peligro en el retraso;*

La localización de sospechosos y el suministro de información de carácter jurídico en casos de urgencia o de peligro en el retraso.”

Artículo 21.- Después del artículo 499, incorpórese la siguiente sección:

“SECCIÓN SEGUNDA

Pruebas Digitales

Art. 499. 1. - Aseguramiento de datos.

- a. *La o el juzgador, de oficio o a petición de parte, podrá ordenar a una o varias personas naturales o jurídicas que aseguren o conserven contenido digital, almacenados en un sistema informático o en un dispositivo de almacenamiento informático, que estén bajo su disposición o control, cuando tenga motivos para sospechar que los datos pueden ser alterados o suprimidos. La orden deberá especificar los datos concretos que se pretende conservar y la medida ordenada no podrá exceder de noventa días, prorrogables por igual período si se mantienen los motivos que fundamentaron la orden.*
- b. *La persona requerida deberá procurar los medios necesarios para preservar de inmediato los datos en cuestión y queda obligado a mantener secreto de la orden recibida durante el tiempo que dure la medida, bajo el apercibimiento de incurrir en responsabilidad penal.*
- c. *El proveedor de servicios de una comunicación que haya recibido la orden de aseguramiento de datos relativos al tráfico de una comunicación informará de inmediato a la autoridad que emitió la orden cuando advierta que la comunicación bajo investigación ha sido efectuada con la participación de otros proveedores de servicios a fin de que se puedan arbitrar las medidas necesarias para solicitar a dichos proveedores el aseguramiento de los datos. No obstante, el proveedor de servicios deberá conservar el contenido digital y los*

datos de tráfico que reposen en su poder, por al menos setenta y dos horas o hasta que la autoridad judicial así lo requiera.

- d. A fin de evitar que el contenido digital sea alterado o manipulado, se procederá conforme las reglas de la investigación de contenido digital, establecidas en este Código.*

Art. 499. 2. - Orden de presentación.

1. La o el juzgador, de oficio o a petición de parte, cuando la naturaleza del contenido digital así lo requiera, podrá ordenar a cualquier persona natural o jurídica, que presente, remita o entregue cualquier contenido digital alojado en un sistema informático que este bajo su poder o control y que se vinculen con la investigación de un delito concreto.

2. Asimismo, la o el juzgador, de oficio o a petición de parte, podrá ordenar a toda persona natural o jurídica que preste un servicio relacionado con cualquiera de las tecnologías de la información y comunicación, o con proveedores de servicios o plataformas digitales que presten sus servicios en el territorio de Ecuador, la entrega del contenido digital que considere necesario, así como los datos de los usuarios o abonados o los datos de identificación y facturación con los que cuente. Para dicho efecto, estos proveedores de servicios o plataformas digitales, deberán designar inmediatamente un representante dentro del territorio ecuatoriano, que estará a cargo de brindar una comunicación más ágil entre las partes, así como todas las facilidades necesarias durante todo el proceso, hasta cuando así lo requiera la o el juzgador.

3. Las ordenes podrán contener la indicación de que la medida deberá mantenerse en secreto bajo el apercibimiento de responsabilidad penal.

Art. 499. 3. - Búsqueda e incautación de contenido digital.

1. La o el juzgador, de oficio o a petición de parte, podrá ordenar el registro de un sistema informático o de una parte de éste, o de un medio de almacenamiento de contenido digital, con el objeto de:

- a. *Incautar los componentes físicos del sistema y, si fuera necesario, los dispositivos para su lectura;*
- b. *Obtener copia forense en legal y debida forma, de los datos en un soporte autónomo; o,*
- c. *Preservar por medios tecnológicos, electrónicos o digitales, los datos de interés para la investigación.*

Regirán en cuanto sean aplicables las normas generales y las mismas limitaciones dispuestas para el secuestro de documentos y correspondencia epistolar.

2. En los supuestos en los que durante la ejecución de una medida de registro e incautación de datos de un sistema informático previstos en el párrafo anterior surjan elementos que permitan considerar que los datos buscados se encuentran almacenados en otro dispositivo o sistema Informático al que se tiene acceso lícito desde el dispositivo o sistema inicial, quienes llevan adelante la medida podrán extenderla o ampliar el registro al otro sistema. La ampliación del registro a los fines de la incautación de datos deberá ser autorizada por el juez salvo que estuviera prevista en la orden original.

Art. 499. 4. – Investigación de contenido digital. – *En la investigación de contenido digital se seguirán las siguientes reglas:*

- 1. El análisis, valoración, recuperación y presentación del contenido digital almacenado en dispositivos o sistemas informáticos se realizará a través de técnicas digitales forenses.*
- 2. Cuando el contenido digital se encuentre almacenado en sistemas y memorias volátiles o equipos tecnológicos que formen parte de la infraestructura crítica del sector público o privado, se realizará su recolección, en el lugar y en tiempo real, con técnicas digitales forenses para preservar su integridad, se aplicará la cadena de custodia y se facilitará su posterior valoración y análisis de contenido.*

3. *Cuando el contenido digital se encuentre almacenado en medios no volátiles, se realizará su recolección, con técnicas digitales forenses para preservar su integridad, se aplicará la cadena de custodia y se facilitará su posterior valoración y análisis de contenido.*
4. *Cuando se recolecte cualquier medio físico que almacene, procese o transmita contenido digital durante una investigación, registro o allanamiento, se deberá identificar e inventariar cada objeto individualmente, fijará su ubicación física con fotografías y un plano del lugar, se protegerá a través de técnicas digitales forenses y se trasladará mediante cadena de custodia a un centro de acopio especializado para este efecto.”*

Artículo 22.- Suprímase el artículo 500.

Artículo 23.- Sustitúyese en el Capítulo Tercero “Medios de prueba”, del Título IV “Prueba”, del Libro Segundo “Procedimiento”, lo siguiente:

- a. *“Sección Segunda: El testimonio” por “Sección Tercera: El testimonio”.*
- b. *“Parágrafo Tercero: La pericia” por “Sección Cuarta: La pericia”.*

DISPOSICIONES TRANSITORIAS

PRIMERA: En un plazo de 30 días contados a partir de la publicación de la presente Ley en el Registro Oficial, la Policía Nacional del Ecuador, la Fiscalía General del Estado y el Consejo de la Judicatura, diseñarán e implementarán un Plan Nacional de Políticas Públicas encaminado a difundir, socializar y capacitar a la ciudadanía a utilizar las tecnologías de forma segura conociendo sus derechos frente a cualquier riesgo o acto de violencia y sobre las disposiciones contenidas en la presente Ley, que permitan promover el derecho a vivir una vida libre de violencia y auto determinada, tanto online como offline, prevenir y

combatir efectivamente la violencia sexual digital, así como fortalecer la lucha contra los delitos informáticos.

SEGUNDA: En un plazo de 30 días contados a partir de la publicación de la presente Ley en el Registro Oficial, el Ministerio de Salud Pública diseñará e implementará campañas de sensibilización y concienciación dirigidas a la ciudadanía, sobre los peligros de la violencia sexual digital y todo tipo de violencia cometida en el entorno digital y el riesgo de los delitos informáticos, así como sobre los derechos vulnerados y sus consecuencias, en virtud de que estos factores acarrearán graves repercusiones en la salud mental y terminan convirtiéndose en una alarma de salud pública.

TERCERA: En un plazo de 180 días contados a partir de la publicación de la presente Ley en el Registro Oficial, la Autoridad Educativa Nacional y la Autoridad rectora de la Educación Superior, deberán incluir en sus mallas curriculares o programas académicos, asignaturas que permitan promover una cultura saludable de consentimiento, el derecho a una vida libre de violencia y auto determinada, tanto online como offline, prevenir y combatir efectivamente la violencia sexual digital y todo tipo de estereotipos y tabús propios de la cultura de la violación, así como fortalecer la lucha contra los delitos informáticos, campañas de sensibilización y concienciación y materiales educativos dirigidos a la comunidad educativa, orientados no solo en riesgos para las mujeres, sino en el contraste de la cultura patriarcal en la producción de violencia, promoviendo acciones educativas y culturales con enfoque de interseccionalidad, inclusivas, paritarias y correlativas, especialmente cuando sean cometidos contra mujeres, minorías y grupos de atención prioritaria.

DISPOSICIÓN REFORMATORIA

ÚNICA. – En la Ley Orgánica Integral para Prevenir y Erradicar la Violencia Contra las Mujeres, realícese las siguientes reformas:

1. En el artículo 10 “Tipos de violencia”, luego del literal g) agréguese lo siguiente:

*“h) **Violencia Sexual Digital.** - Es toda acción que implique principalmente la vulneración o restricción del derecho a la intimidad, realizada contra las mujeres en el entorno digital, a través de cualquiera de las tecnologías de la información y comunicación, mediante la utilización de contenido de carácter personal o íntimo, que contenga la representación visual de desnudos, semidesnudos, o actitudes sexuales que la mujer le hubiese confiado de su intimidad o que hubiese sido obtenido por cualquier otro medio.*

Se entenderá por Tecnologías de la Información y la Comunicación, al conjunto de recursos tecnológicos, utilizados de manera integrada, para el procesamiento, administración y difusión de la información a través de soportes diseñados para ello.

*i) **Violencia mediática.** - Aquella violencia cometida por una persona o grupo de personas a través de la publicación o difusión de información o contenido audiovisual o digital estereotipado, a través de cualquier medio de comunicación público, privado o comunitario que, de manera directa o indirecta, legitime la desigualdad de trato o construya patrones socioculturales reproductores o generadores de desigualdad, discriminación, cosificación, estigmatización o violencia contra las mujeres o en sus relaciones sociales, normalizando así, la subordinación de estas en la sociedad, será sancionada con pena privativa de libertad de uno a tres años.”*

2. En el artículo 25, sustitúyase la letra s), por las siguientes:

“s) Promover en todas las instituciones educativas, la implementación de campañas de educación y promoción de la igualdad de género y respeto

hacia la libertad sexual de la mujer; educación sexual y socio-emotiva con expertos y expertas a partir de una edad joven; educación cívica digital para promover un uso más positivo y consciente de las plataformas digitales, considerando que estas últimas no son neutrales y requieren conocimiento cívico por ser utilizadas con respeto por parte de los ciudadanos.

t) Las demás que establezca la normativa vigente.”

3. Luego del artículo 39, agréguese el siguiente artículo:

“Art. 39.1.- Atribuciones especiales de las entidades nacionales y locales que integran el Sistema Nacional Integral para la Prevención y Erradicación de la Violencia Contra las Mujeres, respecto a la violencia sexual digital y otros tipos de violencia en el entorno digital:

- a. Establecer acciones para prevenir la violencia sexual digital y otros tipos de violencia en el entorno digital que se presenta a través de las tecnologías de la información y comunicación;*
- b. Fortalecer las normativas penal y civil para asegurar la sanción a quienes realizan violencia sexual digital y otros tipos de violencia en el entorno digital;*
- c. Promover y difundir en la sociedad información destinada a prevenir y combatir la violencia sexual digital y otros tipos de violencia en el entorno digital;*
- d. Desarrollar acciones coordinadas de carácter interinstitucional y multidisciplinario, cuya visión y ejercicio se fundamente en la perspectiva de género, con miras a dar atención y seguimiento en la materia a las víctimas de violencia sexual digital y otros tipos de violencia en el entorno digital;*
- e. Suministrar atención psicológica y jurídica, gratuita y especializada a las víctimas de violencia sexual digital y otros tipos de violencia en el entorno digital.”*

DISPOSICIÓN FINAL. - Esta Ley entrará en vigencia a partir de su publicación en el Registro Oficial.

Dado y suscrito en la sede de la Asamblea Nacional, ubicada en el Distrito Metropolitano de Quito, provincia de Pichincha, a los ...

11. RESOLUCIÓN

Por las motivaciones constitucionales y jurídicas expuestas, en la continuación de la Sesión ordinaria virtual No. 165, de fecha 30 de abril de 2021, el Pleno de la Comisión Especializada Permanente de Justicia y Estructura del Estado de la Asamblea Nacional **RESUELVE: APROBAR** por unanimidad el presente Informe para Segundo Debate del “**PROYECTO DE LEY ORGÁNICA REFORMATORIA DEL CÓDIGO ORGÁNICO INTEGRAL PENAL PARA PREVENIR Y COMBATIR LA VIOLENCIA SEXUAL DIGITAL Y FORTALECER LA LUCHA CONTRA LOS DELITOS INFORMÁTICOS**”, con doce (12) votos a favor, cero (0) abstenciones, cero (0) votos en contra, de doce (12) asambleístas presentes, conforme se detalla a continuación:

Tabla No. 10
DETALLE DE LA VOTACIÓN

Asambleísta	Votación
José Ricardo Serrano Salgado	A FAVOR
Kharla del Rocío Chávez Bajaña	A FAVOR
Carlos Urel Ortega Álvarez	A FAVOR
Henry Eduardo Cucalón Camacho	A FAVOR
Luis Esteban Torres Cobo	A FAVOR
María de Lourdes Cuesta Orellana	A FAVOR
Elio Germán Peña Ontaneda	A FAVOR
Rodrigo Collaguazo Pilco	A FAVOR
Rosa Gina Orellana Román	A FAVOR
Héctor Patricio Muñoz Alarcón	A FAVOR
Franklin Omar Samaniego Maigua	A FAVOR
Karla Gabriela Cadena Vélez	A FAVOR

12. ASAMBLEÍSTA PONENTE

Asambleísta José Ricardo Serrano Salgado, Presidente de la Comisión Especializada Permanente de Justicia y Estructura del Estado de la Asamblea Nacional.

13. NOMBRE Y FIRMA DE LOS ASAMBLEÍSTAS QUE CONOCIERON Y SUSCRIBIERON EL INFORME



Firmado electrónicamente por:
**JOSE RICARDO
SERRANO SALGADO**

José Ricardo Serrano Salgado

PRESIDENTE

**Comisión Especializada Permanente
De Justicia y Estructura del Estado**

Kharla del Rocío Chávez Bajaña

VICEPRESIDENTA

**Comisión Especializada Permanente
De Justicia y Estructura del Estado**



Firmado electrónicamente por:
**CARLOS UREL
ORTEGA
ALVAREZ**

Carlos Urel Ortega Alvarez

ASAMBLEÍSTA



Firmado electrónicamente por:
**HENRY EDUARDO
CUCALON CAMACHO**

Henry Eduardo Cucalón Camacho

ASAMBLEÍSTA



Firmado electrónicamente por:
**LUIS ESTEBAN
TORRES COBO**

Luis Esteban Torres Cobo
ASAMBLEÍSTA



Firmado electrónicamente por:
**MARIA DE LOURDES
CUESTA ORELLANA**

María de Lourdes Cuesta Orellana
ASAMBLEÍSTA



Firmado electrónicamente por:
**ELIO GERMAN
PENA ONTANEDA**

Elio Germán Peña Ontaneda
ASAMBLEÍSTA



Firmado electrónicamente por:
**RODRIGO
COLLAGUAZO**

Rodrigo Collaguazo Pilco
ASAMBLEÍSTA



Firmado electrónicamente por:
**ROSA GINA
ORELLANA**

Rosa Gina Orellana Román
ASAMBLEÍSTA



Firmado electrónicamente por:
**KARLA
GABRIELA
CADENA VELEZ**

Héctor Patricio Muñoz Alarcón
ASAMBLEÍSTA



Firmado electrónicamente por:
**FRANKLIN OMAR
SAMANIEGO
MAIGUA**

Franklin Omar Samaniego Maigua
ASAMBLEÍSTA

Karla Gabriela Cadena Vélez
ASAMBLEÍSTA

14. CERTIFICACIÓN:

En mi calidad de Secretaria Relatora de la Comisión Especializada Permanente de Justicia y Estructura del Estado, **CERTIFICO:** Que, el Informe para Segundo Debate del “Proyecto de Ley Orgánica Reformatoria del Código Orgánico Integral Penal para Prevenir y Combatir la Violencia Sexual Digital y Fortalecer la Lucha contra los Delitos Informáticos”, fue conocido, debatido y aprobado por unanimidad en la Sesión ordinaria virtual No. 165 de la Comisión Especializada Permanente de Justicia y Estructura del Estado, celebrada el día viernes, 30 de abril de 2021.

Dado y suscrito en el D.M. de Quito, a los 30 días del mes de abril de 2021, lo certifico.-

Dra. Nathalia Jaramillo Del Pozo
SECRETARIA RELATORA
COMISIÓN ESPECIALIZADA PERMANENTE
DE JUSTICIA Y ESTRUCTURA DEL ESTADO

15. BIBLIOGRAFÍA:

- Álvarez, A., Gómez, C., y Sierra, C. (2020). Typologies of sexual double standard adherence in Spanish population.
- Álvarez, M. (2014). Acceso a la justicia. *Revista de Investigaciones Jurídicas*.
- AP NEWS. 2018. US Open aclara norma tras sanción a Alize Cornet. [online] Disponible en: <https://apnews.com/article/36133b9b01ea49a8955b5c5ebf2adc13>
- BBC News Mundo. 2018. La tenista Alizé Cornet se saca la camiseta y la sancionan: la polémica machista del Abierto de Estados Unidos - BBC News Mundo. [online] Disponible en: <https://www.bbc.com/mundo/deportes-45350685>
- Bogle, K. (2008). *Hooking up: Sex, dating, and relationships on campus*. United State of America: New York Press
- Calderón, C., & Quishpe Reinoso, A. M. (2020). El ciberacoso en niños, niñas y adolescentes (Bachelor's thesis, Quito: UCE).
- Caramonte, M. (2002). El cuerpo colonizado. *Asparkía: investigació feminista*, 103-114.
- Cobo, E. (2015). El cuerpo de las mujeres y la sobrecarga de sexualidad. *Investigaciones Feministas*, 6, 7–19. Disponible en <http://revistas.ucm.es/index.php/INFE/article/view/51376/4765>
- Convención Americana sobre Derechos Humanos suscrita en la Conferencia Especializada Interamericana sobre Derechos Humanos. (1969) San José, P. Recuperado de https://www.oas.org/dil/esp/tratados_b-32_convencion_americana_sobre_derechos_humanos.html.
- Convención interamericana para prevenir, sancionar y erradicar la violencia contra la mujer. (1994). Convención de BELEM DO PARA. file:///C:/Users/Hp/AppData/Local/Temp/M-0840-C.pdf.
- Convención para la eliminación de todas las formas de discriminación contra la mujer "CEDAW". (2011).
- Convenio de Budapest. Unión Europea, Bruselas, Bélgica, 1 de julio de 2004.
- Coral, A. (2010). El cuerpo femenino sexualizado: entre las construcciones de género y la Ley de Justicia y Paz. *International Law*, (17), 381-409.
- Corte Constitucional del Ecuador. (27 de enero de 2021). Sentencia 2064-14-EP/21. [MP Carmen Corral].
- Declaración Universal de los Derechos humanos. (1948). Asamblea General de las Naciones Unidas.
- Declaración y Plataforma de acción de Beijing, Beijing, 15 de septiembre de 1995.
- Diario Semana. (21 de septiembre de 2020). Anuncian investigación internacional para atrapar a pedófilos que usan la red TikTok. Disponible en <https://www.semana.com/nacion/articulo/anuncian-investigacion-internacional-para-atrapar-a-pedofilos-que-usan-la-red-tiktok/202042/>
- El Comercio. (24 de septiembre de 2020). ¿Qué rastro deja el número telefónico que contactó a una niña usuaria de TikTok?; Ecuador es punto de pornografía infantil. Disponible en

- https://www.elcomercio.com/actualidad/telefono-grooming-ecuador-colombia-tiktok.html?fbclid=IwAR2vslxapLcUq3HYS-XBOioWjVQNOQVhwV3_3rMhuaHQIDfIVBhP5yIE111
- El Espectador. (21 de septiembre de 2020). Denuncia de una colombiana destapó red de pedofilia en TikTok. Disponible en <https://www.elespectador.com/noticias/nacional/red-de-pedofilia-en-tiktok-usan-el-perfil-falso-de-karol-sevilla/>
 - El Tiempo. (20 de septiembre de 2020). El drama de una familia en Medellín por red de pedofilia en TikTok. Disponible en <https://www.eltiempo.com/colombia/medellin/red-de-pedofilos-contactaron-a-nina-de-9-anos-en-medellin-por-tik-tok-538837>
 - Fidler, R. (1998). *Mediamorfosis, comprender los nuevos medios*. Buenos Aires: Gránica.
 - Fredrickson, B. L. y Roberts, T. A. (1997). Objectification theory: Toward understanding women's lived experiences and mental health risks. *Psychology of Women Quarterly*, 21, 173-206.
 - García, D. y Cabello, S. (Eds.). (2013). *Actualizaciones en sexología Clínica y Educativa*. España: Universidad de Huelva.
 - Ley N° 27590. Buenos Aires, Argentina, 16 de diciembre de 2020.
 - Ley Orgánica Integral para Prevenir y Erradicar la Violencia contra las Mujeres. (2018). <https://biblioteca.defensoria.gob.ec/handle/37000/2716>.
 - Luzuriaga, G. (2017). *Delitos informáticos: la virtual realidad*. Quito: Offset Chávez. 232pp. ISBN: 978-9942-28-322.1.
 - Metro Ecuador. (22 de septiembre de 2020). Desde un número de Ecuador red de pedofilia escribía a una niña en Colombia; TikTok fue el primer acercamiento. Disponible en <https://www.metroecuador.com.ec/ec/noticias/2020/09/22/numero-ecuador-red-pedofilia-tiktok.html>
 - Milhausen, R. y Herold, S. (2001). Reconceptualizing the sexual double standard. *Journal of Psychology and Human Sexuality*, 13, 63-83. https://dx.doi.org/10.1300/J056v13n02_05
 - Monge, F. (2013). Doble moral sexual y violencia de género. *El Antoniano*, 123(23), 141-146
 - Mundo Deportivo. 2018. Polémica por la sanción a Alizé Cornet por cambiarse de camiseta en el US Open de tenis. [online] Disponible en: <https://www.mundodeportivo.com/tenis/20180829/451531379662/polemica-por-la-sancion-a-cornet-por-cambiarse-de-camiseta-en-la-pista.html>
 - Observación del Comité de los Derechos del Niño “Observación general núm. 25 (2021) sobre los niños derechos en relación con el entorno digital” CRC/C/GC/25 /2 de marzo de 2021).
 - Organización de Estados Americanos. (2019). *Combatir la Violencia en línea contras las mujeres un llamado a la protección*. Vol. 7, 5-24. <https://www.oas.org/es/sms/cicte/docs/20191125-ESP-White-Paper-7-VIOLENCE-AGAINST-WOMEN.pdf>.
 - Organización de las Naciones Unidas. (2015). *Declaración y Plataforma de Acción de Beijing, Declaración política y documentos resultados de Beijing*.

- Organización Panamericana de la Salud para la Organización Mundial de la Salud (2013): Comprender y abordar la violencia contra las mujeres. Violencia sexual. Recuperado de http://apps.who.int/iris/bitstream/665/98821/1/WHO_RHR_12.37_spa.pdf?ua=
- Pacto internacional de derechos civiles y políticos. (1966). <https://www.acnur.org/fileadmin/Documentos/BDL/2004/2845.pdf>.
- Política pública por una internet segura para niños, niñas y adolescentes. Septiembre 2020 (Ecuador).
- Resolución 73/187 de la Asamblea General de la ONU. “Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos”. (30 de julio de 2019), disponible en: https://www.unodc.org/documents/Cybercrime/SG_report/V1908185_S.pdf.
- Sandra Lee Bartky, *Femininity and Domination: Studies in the Phenomenology of Oppression (Thinking Gender)*, 26 (Routledge, New York, 1990).
- Semenzin, S. (2021). *Blockchain & data justice. The political culture of technology* [Tesis de doctorado no publicada]. Universidad de Milán y Universidad de Turín.
- Semenzin, S., y Bainotti, L. (2020). *The Use of Telegram for Non-Consensual Dissemination of Intimate Images: Gendered Affordances and the Construction of Masculinities*. *Social Media+ Society*, 6(4), 2056305120984453. Recuperado de <https://journals.sagepub.com/doi/full/10.1177/2056305120984453>.
- Unicef. (2006). *Convención sobre los Derechos del Niño*.
- Vistazo. (23 de septiembre de 2020). *Alerta por red de pedófilos en TikTok desde un número de Ecuador: escribían a niña en Colombia; su hermana revela cómo operan*. Disponible en <https://www.vistazo.com/seccion/actualidad-mundial/alerta-por-red-de-pedofilos-en-tiktok-desde-un-numero-de-ecuador>
- Yépez, E. (2016). *El grooming y la protección de las niñas, niños y adolescentes en el ordenamiento jurídico ecuatoriano (Bachelor's thesis, Quito: Universidad de las Américas, 2016.)*. <http://dspace.udla.edu.ec/handle/33000/6984>.
- Zaikman, Y. y Marks, M. (2017). *Promoting theory-based perspectives in sexual double standard research*. *Sex Roles*, 76(7-8), 407-420. doi:<http://dx.doi.org/10.1007/s11199-016-0677-z>



Responder

Responder a todos

Reenviar

Archivo

Eliminar

Spam



Acciones ▼



CONFIRMACIÓN VOTO

De: **Kharla Del Rocio Chávez Bajaña**Para: **José Ricardo Serrano Salgado** **Nathalia Verónica Jaramillo del Pozo**CC: **Comisión de Justicia y Estructura del Estado**Babahoyo, **30 de abril** de 2021

Doctor

José Serrano Salgado

Presidente**COMISIÓN DE JUSTICIA Y ESTRUCTURA DEL ESTADO**
ASAMBLEA NACIONALDe **mi** consideración:

Por medio del presente, ratifico **mi** voto afirmativo hacia el Informe del proyecto de Ley Orgánica Reformativa del Código Orgánico Integral Penal y de la Ley Orgánica Integral para Prevenir y Erradicar la Violencia Contra las Mujeres, para Prevenir y Sancionar la Violencia Sexual Digital, aprobado en la Sesión No. 165 de **30 de abril** de 2021 de la Comisión de Justicia y Estructura del Estado de la Asamblea Nacional.

Atentamente,

Ab. Kharla Chávez
Asambleísta Nacional

30 de Abril 2021 17:37



Buscar

Comisión de...l Estado ▼

