Actualizado
03 octubre 2025

LEY DE DELITOS INFORMÁTICOS

LEY Nº 30096

CAPÍTULO I
FINALIDAD Y OBJETO DE LA LEY

Artículo 1. Objeto de la Ley

La presente Ley tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia.

CAPÍTULO II
DELITOS CONTRA DATOS Y SISTEMAS INFORMÁTICOS

Artículo 2. Acceso ilícito

El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, **o se excede en lo autorizado**, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.

Si el agente accede deliberada e ilegítimamente, en todo o en parte, al sistema informático vulnerando las medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa."

(*) Artículo modificado por el Artículo 2 del Decreto Legislativo Nº 1614, publicado el 21 diciembre 2023

Artículo 3. Atentado a la integridad de datos informáticos

El que deliberada e ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.**”**

“ Artículo 4. Atentado a la integridad de sistemas informáticos

El que deliberada e ilegítimamente inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.**”**

CAPÍTULO III
DELITOS INFORMÁTICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES

“Artículo 5. Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos

El que a través de internet u otro medio análogo contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para proponerle llevar a cabo

cualquier acto de connotación sexual con él o con tercero, será reprimido con una pena privativa de libertad **no menor de seis ni mayor de nueve años**.

Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años.

(*) Artículo modificado por el Artículo 2 del Decreto Legislativo Nº 1591, publicado el 13 diciembre 2023

"Artículo 5-A.- Chantaje sexual con materiales elaborados o modificados por medios digitales o tecnológicos

El que, mediante el uso de tecnologías de la información o comunicación, amenaza o intimida a una persona, con la difusión de imágenes, materiales audiovisuales o audios elaborados o modificados por medios digitales o tecnológicos, para obtener de ella una conducta o acto de connotación sexual, será reprimido con pena privativa de la libertad no menor de dos ni mayor de cuatro años e inhabilitación, según corresponda, conforme a los incisos 5, 9, 10 y 11 del artículo 36 del Código Penal.

La pena privativa de libertad será no menor de tres ni mayor de cinco años e inhabilitación, cuando concurra cualquiera de las siguientes circunstancias:

1. La amenaza a la víctima se refiere a la difusión de imágenes, materiales audiovisuales o audios con contenido sexual en los que esta aparece o participa.
2. Cuando la víctima mantenga o haya mantenido una relación de pareja con el agente, son o han sido convivientes o cónyuges.
3. Cuando la víctima es menor de 18 años de edad."**(*)**

(*) Artículo incorporado por el Artículo 4 del Decreto Legislativo Nº 1625, publicado el 08 agosto 2024.

CAPÍTULO IV
DELITOS INFORMÁTICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES

" Artículo 7. Interceptación de datos informáticos

El que deliberada e ilegítimamente intercepta datos informáticos en transmisiones no públicas, dirigidos a un sistema informático, originados en un sistema informático o efectuado dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con una pena privativa de libertad no menor de tres ni mayor de seis años.

La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con la Ley 27806, Ley de Transparencia y Acceso a la Información Pública.

La pena privativa de libertad será no menor de ocho ni mayor de diez cuando el delito comprometa la defensa, seguridad o soberanía nacionales.

Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores.**"**

CAPÍTULO V
DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO

"**Artículo 8. Fraude informático**

El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos, **suplantación de interfaces o páginas web** o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será

reprimido con una pena privativa de libertad no menor de **cuatro** ni mayor de **ocho** años y con sesenta a ciento veinte días-multa.

La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social.

La misma pena se aplica al que intencionalmente colabora con la comisión de alguno de los supuestos de los párrafos precedentes, facilitando la transferencia de activos."

"**Artículo 8-A. Préstamos informáticos extorsivos**

El que a través de plataformas digitales, internet u otro medio análogo induce u obliga mediante amenaza, intimidación, engaño o ardid a aceptar dinero o bienes, simulando un contrato de mutuo o cualquier otro con el fin de obtener una ventaja indebida, será reprimido con pena privativa de libertad no menor de diez ni mayor de quince años.

La pena será no menor de quince ni mayor de veinticinco años, cuando:

a) Se ejerce violencia para obtener la ventaja indebida.
b) La víctima tiene discapacidad, tiene entre catorce y menos de dieciocho años de edad o es adulta mayor, padece de una enfermedad grave, pertenece a un pueblo indígena u originario, o presenta cualquier situación de vulnerabilidad.
c) El agente comete el delito en el marco de la actividad de una persona jurídica.
d) La comisión del hecho punible es de carácter transnacional, de acuerdo al numeral 2 del artículo 3 de la Convención de las Naciones Unidas Contra la Delincuencia Organizada Transnacional - Convención de Palermo".**(*)**

(*) Artículo incorporado por el Artículo 2 de la Nº 32183, publicada el 11 diciembre 2024.

CAPÍTULO VI
DELITOS INFORMÁTICOS CONTRA LA FE PÚBLICA

Artículo 9. Suplantación de identidad

El que, mediante las tecnologías **digitales** suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material, moral **o de cualquier otra índole**, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.

La pena privativa de libertad es no menor de seis ni mayor de nueve años cuando se suplante la identidad de una persona menor de 18 años de edad y resulte algún perjuicio, material, moral o de cualquier otra índole."

(*) Artículo modificado por el Artículo 2 del Decreto Legislativo Nº 1591, publicado el 13 diciembre 2023

"**Artículo 9-A.- Activación de una SIM Card o de una línea de servicio móvil sin consentimiento del titular**

El que, mediante sistemas informáticos u otro mecanismo, active una SIM Card o una línea de servicio móvil en la plataforma de abonados de una empresa operadora sin el consentimiento del titular, o cuando la información proporcionada del titular sea falsa o errónea, será reprimido con pena privativa de libertad no menor de cuatro ni mayor de ocho años y con inhabilitación conforme al numeral 4 del artículo 36 del Código Penal". (*)

(*) Articulo incorporado por la Ley 32451, publicado el 30 de setiembre del 2025, en el Diario Oficial El Peruano

CAPÍTULO VII
DISPOSICIONES COMUNES

Artículo 10. Abuso de mecanismos y dispositivos informáticos

El que deliberada e ilegítimamente fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización, uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley, o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.**"**

Artículo 11. Agravantes

El juez aumenta la pena privativa de libertad hasta en un tercio por encima del máximo legal fijado para cualquiera de los delitos previstos en la presente Ley cuando:

1. El agente comete el delito en calidad de integrante de una organización criminal.

2. El agente comete el delito mediante el abuso de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función.

3. El agente comete el delito con el fin de obtener un beneficio económico, salvo en los delitos que prevén dicha circunstancia.

4. El delito compromete fines asistenciales, la defensa, la seguridad y la soberanía nacionales.
5. El agente comete el delito empleando la inteligencia artificial o tecnologías similares o análogas". **(*) Literal incorporado por la Ley 32314 publicada el 29 de abril del 2025**

Artículo 12. Exención de responsabilidad penal

Está exento de responsabilidad penal el que realiza las conductas descritas en los artículos 2, 3, 4 y 10 con el propósito de llevar a cabo pruebas autorizadas u otros procedimientos autorizados destinados a proteger sistemas informáticos.**" (*)**
(*) Artículo incorporado por el Artículo 3 de la Ley N° 30171, publicada el 10 marzo 2014**.**

"Artículo 12-A.- Adquisición, posesión y tráfico ilícito de datos informáticos

El que posee, compre, recibe, comercialice, vende, facilite, intercambie o trafique datos informáticos, credenciales de acceso o bases de datos personales, teniendo conocimiento o debiendo presumir que se obtuvo sin consentimiento de su titular o mediante la vulneración de sistemas de seguridad o la comisión de un delito informático, es reprimido

con pena privativa de libertad no menor de cinco (5) ni mayor de ocho (8) años y con ciento ochenta (180) a trescientos sesenta y cinco (365) días-multa.
La pena privativa de libertad es no menor de ocho (8) ni mayor de diez (10) años, e inhabilitación, cuando:

a) El agente actúa como integrante de una organización criminal;
b) Se cause perjuicio patrimonial grave o afectación a una pluralidad de personas; o
c) La base de datos es procesada o custodiada por una entidad pública.

Queda exceptuada de responsabilidad penal la adquisición, posesión, intercambio o tratamiento de datos informáticos cuando estas conductas se realicen con autorización expresa del titular, conforme a la Ley Nº 29733, Ley de Protección de Datos Personales, en cumplimiento de un mandato judicial o administrativo emitido conforme a ley, o en el ejercicio legítimo de derechos fundamentales, funciones legalmente reconocidas, **o actividades desarrolladas en los sectores bursátil, financiero, previsional o de seguros**, **siempre que no exista finalidad de aprovechamiento ilícito o de comercialización indebida de la información**."(**)

(*) Artículo incorporado por el Artículo 3 del Decreto Legislativo, publicada el 24 de enero del 2026, en el Diario Oficial El Peruano.
(**) 3er. Párrafo modificado por el Decreto Legislativo 1741, publicado el 13 de febrero del 2026, en el Diario Oficial El Peruano.

DISPOSICIONES COMPLEMENTARIAS FINALES

PRIMERA. Codificación de la pornografía infantil

La Policía Nacional del Perú puede mantener en sus archivos, con la autorización y supervisión respectiva del Ministerio Público, material de pornografía infantil, en medios de almacenamiento de datos informáticos, para fines exclusivos del cumplimiento de su función. Para tal efecto, cuenta con una base de datos debidamente codificada.

La Policía Nacional del Perú y el Ministerio Público establecen protocolos de coordinación en el plazo de treinta días a fin de cumplir con la disposición establecida en el párrafo anterior.

"SEGUNDA.- Agente encubierto en delitos informáticos

El fiscal, atendiendo a la urgencia del caso particular y con la debida diligencia, puede autorizar la actuación de agentes encubiertos a efectos de realizar las investigaciones de los delitos previstos en la presente Ley y de todo delito que se cometa mediante tecnologías de la información o de la comunicación, **incluso si estas acciones deben realizarse en entornos digitales,** y con prescindencia de si los mismos están vinculados a una organización criminal, de conformidad con el artículo 341 del Código Procesal Penal, aprobado mediante el Decreto Legislativo 957.

Los protocolos para la actuación del agente encubierto en entornos digitales, tanto en el marco de la presente Ley, como en el marco del artículo 341 del Código Procesal Penal, aprobado mediante el Decreto Legislativo 957, son coordinados, en cuanto corresponda, con la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en concordancia con las normas vigentes que regulan el Sistema Nacional de Transformación Digital."

(*) Disposición modificada por el Artículo 2 del Decreto Legislativo Nº 1591, publicado el 13 diciembre 2023

“TERCERA. Coordinación interinstitucional entre la Policía Nacional, el Ministerio Público y otros organismos especializados

La Policía Nacional del Perú fortalece el órgano especializado encargado de coordinar las funciones de investigación con el Ministerio Público. A fin de establecer mecanismos de comunicación con los órganos de gobierno del Ministerio Público, la **Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros** y los Organismos Especializados de las Fuerzas Armadas, la Policía Nacional centraliza la información aportando su experiencia en la elaboración de los programas y acciones para la adecuada persecución de los delitos informáticos, y desarrolla programas de protección y seguridad.”

(*) Disposición modificada por el Artículo 2 del Decreto Legislativo Nº 1591, publicado el 13 diciembre 2023

“ CUARTA. Cooperación operativa

Con el objeto de garantizar el intercambio de información, los equipos de investigación conjuntos, la transmisión de documentos, la interceptación de comunicaciones y demás actividades correspondientes para dar efectividad a la presente Ley, la Policía Nacional del Perú, el Ministerio Público, el Poder Judicial, el Pe-CERT (Centro de respuesta temprana del gobierno para ataques cibernéticos), la ONGEI (Oficina Nacional de Gobierno Electrónico e Informática), Organismos Especializados de las Fuerzas Armadas y los operadores del sector privado involucrados en la lucha contra los delitos informáticos deben establecer protocolos de cooperación operativa reformada en el plazo de treinta días desde la vigencia de la presente Ley.**”**

QUINTA. Capacitación

Las instituciones públicas involucradas en la prevención y represión de los delitos informáticos deben impartir cursos de capacitación destinados a mejorar la formación profesional de su personal -especialmente de la Policía Nacional del Perú, el Ministerio Público y el Poder Judicial- en el tratamiento de los delitos previstos en la presente Ley.

SEXTA. Medidas de seguridad

La Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) promueve permanentemente, en coordinación con las instituciones del sector público, el fortalecimiento de sus medidas de seguridad para la protección de los datos informáticos sensibles y la integridad de sus sistemas informáticos.

SÉTIMA. Buenas prácticas

El Estado peruano realiza acciones conjuntas con otros Estados a fin de poner en marcha acciones y medidas concretas destinadas a combatir el fenómeno de los ataques masivos contra las infraestructuras informáticas y establece los mecanismos de prevención necesarios, incluyendo respuestas coordinadas e intercambio de información y buenas prácticas.

OCTAVA. Convenios multilaterales

El Estado peruano promueve la firma y ratificación de convenios multilaterales que garanticen la cooperación mutua con otros Estados para la persecución de los delitos informáticos.

NOVENA. Terminología

Para efectos de la presente Ley, se entenderá, de conformidad con el artículo 1 del Convenio sobre la Ciberdelincuencia, Budapest, 23.XI.2001:

a.**Por sistema informático:** todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.

b.**Por datos informáticos:** toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función.

DÉCIMA. Regulación e imposición de multas por la Superintendencia de Banca, Seguros y AFP

La Superintendencia de Banca, Seguros y AFP establece la escala de multas atendiendo a las características, complejidad y circunstancias de los casos aplicables a las empresas bajo su supervisión que incumplan con la obligación prevista en el numeral 5 del artículo 235 del Código Procesal Penal, aprobado por el Decreto Legislativo 957.

El juez, en el término de setenta y dos horas, pone en conocimiento del órgano supervisor la omisión incurrida por la empresa, con los recaudos correspondientes sobre las características, complejidad y circunstancias del caso particular, a fin de aplicarse la multa correspondiente.

UNDÉCIMA. Regulación e imposición de multas por el Organismo Supervisor de Inversión Privada en Telecomunicaciones

El Organismo Supervisor de Inversión Privada en Telecomunicaciones establece la escala de multas atendiendo a las características, complejidad y circunstancias de los casos aplicables a las empresas bajo su supervisión que incumplan con la obligación prevista en el numeral 4 del artículo 230 del Código Procesal Penal, aprobado por el Decreto Legislativo 957.

*El juez, en el término de setenta y dos horas, pone en conocimiento del órgano supervisor la omisión incurrida por la empresa, con los recaudos correspondientes sobre las características, complejidad y circunstancias del caso particular, a fin de aplicarse la multa correspondiente.***(*)**

(*) Disposición modificada por el Artículo 2 de la Ley N° 30171, publicada el 10 marzo 2014**, cuyo texto es el siguiente:**

“ UNDÉCIMA. Regulación e imposición de multas por el Organismo Supervisor de Inversión Privada en Telecomunicaciones

El Organismo Supervisor de Inversión Privada en Telecomunicaciones establece las multas aplicables a las empresas bajo su supervisión que incumplan con la obligación prevista en el numeral 4 del artículo 230 del Código Procesal Penal, aprobado por Decreto Legislativo 957.

Las empresas de telecomunicaciones organizan sus recursos humanos y logísticos a fin de cumplir con la debida diligencia y sin dilación la obligación prevista en el numeral 4 del artículo 230 del Código Procesal Penal.

El juez, en el término de setenta y dos horas, pone en conocimiento del órgano supervisor la omisión incurrida por la empresa a fin de que el Organismo Supervisor de

Inversión Privada en Telecomunicaciones aplique la multa correspondiente.**”**

DISPOSICIONES COMPLEMENTARIAS MODIFICATORIAS

PRIMERA. Modificación de la Ley 27697, Ley que otorga facultad al fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional

Modifícase el artículo 1 de la Ley 27697, Ley que otorga facultad al fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional, modificado por el Decreto Legislativo 991 y por Ley 30077, en los siguientes términos:(*) RECTIFICADO POR FE DE ERRATAS

“**Artículo 1. Marco y finalidad**

La presente Ley tiene por finalidad desarrollar legislativamente la facultad constitucional otorgada a los jueces para conocer y controlar las comunicaciones de las personas que son materia de investigación preliminar o jurisdiccional.

Solo podrá hacerse uso de la facultad prevista en la presente Ley en los siguientes delitos:

1. Secuestro.
2. Trata de personas.
3. Pornografía infantil.
4. Robo agravado.
5. Extorsión.
6. Tráfico ilícito de drogas.
7. Tráfico ilícito de migrantes.
8. Delitos contra la humanidad.
9. Atentados contra la seguridad nacional y traición a la patria.
10. Peculado.
11. Corrupción de funcionarios.
12. Terrorismo.
13. Delitos tributarios y aduaneros.
14. Lavado de activos.
15. Delitos informáticos.”

SEGUNDA. Modificación de la Ley 30077, Ley contra el crimen organizado

Modifícase el numeral 9 del artículo 3 de la Ley 30077, Ley contra el crimen organizado, en los siguientes términos:

“**Artículo 3. Delitos comprendidos**

La presente Ley es aplicable a los siguientes delitos:

(...)

9. Delitos informáticos previstos en la ley penal.”**(*)**

(*) Confrontar con el Artículo 4 del Decreto Legislativo N° 1244, publicado el 29 octubre 2016.

TERCERA. Modificación del Código Procesal Penal

Modifícase el numeral 4 del artículo 230, el numeral 5 del artículo 235 y el literal a) del numeral 1 del artículo 473 del Código Procesal Penal, aprobado por Decreto Legislativo 957 y modificado por Ley 30077, en los siguientes términos:(*) RECTIFICADO POR FE

DE ERRATAS

"**Artículo 230. Intervención o grabación o registro de comunicaciones telefónicas o de otras formas de comunicación**

(...)

4. Los concesionarios de servicios públicos de telecomunicaciones deberán facilitar, en el plazo máximo de treinta días hábiles, la geolocalización de teléfonos móviles y la diligencia de intervención, grabación o registro de las comunicaciones, así como la información sobre la identidad de los titulares del servicio, los números de registro del cliente, de la línea telefónica y del equipo, del tráfico de llamadas y los números de protocolo de internet, que haya sido dispuesta mediante resolución judicial, en tiempo real y en forma ininterrumpida, las veinticuatro horas de los trescientos sesenta y cinco días del año, bajo apercibimiento de ser pasible de las responsabilidades de ley en caso de incumplimiento. Los servidores de las indicadas empresas deberán guardar secreto acerca de las mismas, salvo que se les citare como testigos al procedimiento. El juez fija el plazo en atención a las características, complejidad y circunstancias del caso en particular.

Dichos concesionarios otorgarán el acceso, la compatibilidad y conexión de su tecnología con el Sistema de Intervención y Control de las Comunicaciones de la Policía Nacional del Perú. Asimismo, cuando por razones de innovación tecnológica los concesionarios renueven sus equipos o software, se encontrarán obligados a mantener la compatibilidad con el Sistema de Intervención y Control de las Comunicaciones de la Policía Nacional del Perú.**(*)**

(*) Confrontar con el Artículo 6 de la Ley N° 30171, publicada el 10 marzo 2014.

Artículo 235. Levantamiento del secreto bancario

(...)

5. Las empresas o entidades requeridas con la orden judicial deberán proporcionar, en el plazo máximo de treinta días hábiles, la información correspondiente o las actas y documentos, incluso su original, si así se ordena, y todo otro vínculo al proceso que determine por razón de su actividad, bajo apercibimiento de las responsabilidades establecidas en la ley. El juez fija el plazo en atención a las características, complejidad y circunstancias del caso en particular.

Artículo 473. Ámbito del proceso y competencia

1. Los delitos que pueden ser objeto de acuerdo, sin perjuicio de los que establezca la Ley, son los siguientes:

a) Asociación ilícita, terrorismo, lavado de activos, delitos informáticos, contra la humanidad;"**(*)**

(*) Confrontar con el Artículo 2 del Decreto Legislativo N° 1301, publicado el 30 diciembre 2016**, el mismo que entró en vigencia a nivel nacional a los noventa (90) días contados a partir del día siguiente de su publicación en el Diario Oficial El Peruano.**

CUARTA. Modificación de los artículos 162, 183-A y 323 del Código Penal

Modifícanse los artículos 162, 183-A y 323 del Código Penal, aprobado por el Decreto Legislativo 635, en los siguientes términos:

"**Artículo 162. Interferencia telefónica**
El que, indebidamente, interfiere o escucha una conversación telefónica o similar será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años.

Si el agente es funcionario público, la pena privativa de libertad será no menor de cuatro ni mayor de ocho años e inhabilitación conforme al artículo 36, incisos 1, 2 y 4.

La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con las normas de la materia.

La pena privativa de libertad será no menor de ocho ni mayor de diez años cuando el delito comprometa la defensa, la seguridad o la soberanía nacionales.**(*)**

(*) Confrontar con el Artículo 4 de la Ley N° 30171, publicada el 10 marzo 2014**.**

Artículo 183-A. Pornografía infantil
El que posee, promueve, fabrica, distribuye, exhibe, ofrece, comercializa o publica, importa o exporta por cualquier medio objetos, libros, escritos, imágenes, videos o audios, o realiza espectáculos en vivo de carácter pornográfico, en los cuales se utilice a personas de catorce y menos de dieciocho años de edad, será sancionado con pena privativa de libertad no menor de seis ni mayor de diez años y con ciento veinte a trescientos sesenta y cinco días multa.

La pena privativa de libertad será no menor de diez ni mayor de doce años y de cincuenta a trescientos sesenta y cinco días multa cuando:

1. El menor tenga menos de catorce años de edad.

2. El material pornográfico se difunda a través de las tecnologías de la información o de la comunicación.

Si la víctima se encuentra en alguna de las condiciones previstas en el último párrafo del artículo 173 o si el agente actúa en calidad de integrante de una organización dedicada a la pornografía infantil, la pena privativa de libertad será no menor de doce ni mayor de quince años. De ser el caso, el agente será inhabilitado conforme a los numerales 1, 2 y 4 del artículo 36.**(*)**
(*) Confrontar con el Artículo 1 de la Ley N° 30963, publicada el 18 junio 2019.
Artículo 323. Discriminación
El que, por sí o mediante terceros, discrimina a una o más personas o grupo de personas, o incita o promueve en forma pública actos discriminatorios, por motivo racial, religioso, sexual, de factor genético, filiación, edad, discapacidad, idioma, identidad étnica y cultural, indumentaria, opinión política o de cualquier índole, o condición económica, con el objeto de anular o menoscabar el reconocimiento, goce o ejercicio de los derechos de la persona, será reprimido con pena privativa de libertad no menor de dos años ni mayor de tres o con prestación de servicios a la comunidad de sesenta a ciento veinte jornadas.

Si el agente es funcionario o servidor público, la pena será no menor de dos ni mayor de cuatro años e inhabilitación conforme al numeral 2 del artículo 36.

La misma pena privativa de libertad señalada en el párrafo anterior se impondrá si la discriminación se ha materializado mediante actos de violencia física o mental, o si se

realiza a través de las tecnologías de la información o de la comunicación."**(*)**

(*) Confrontar con el Artículo 4 de la Ley N° 30171, publicada el 10 marzo 2014**.**

DISPOSICIÓN COMPLEMENTARIA DEROGATORIA

ÚNICA. Derogatoria
Deróganse el numeral 4 del segundo párrafo del artículo 186 y los artículos 207-A, 207-B, 207-C y 207-D del Código Penal.(*) RECTIFICADO POR FE DE ERRATAS

Comuníquese al señor Presidente Constitucional de la República para su promulgación.

En Lima, a los veintisiete días del mes de setiembre de dos mil trece.

FREDY OTÁROLA PEÑARANDA
Presidente del Congreso de la República

MARÍA DEL CARMEN OMONTE DURAND
Primera Vicepresidenta del Congreso de la República

AL SEÑOR PRESIDENTE CONSTITUCIONAL DE LA REPÚBLICA

POR TANTO:

Mando se publique y cumpla.

Dado en la Casa de Gobierno, en Lima, a los veintiún días del mes de octubre del año dos mil trece.

OLLANTA HUMALA TASSO
Presidente Constitucional de la República

JUAN F. JIMÉNEZ MAYOR
Presidente del Consejo de Ministros