



TEXTO SUSTITUTORIO

El Congreso de la República
Ha dado la Ley siguiente:

LEY DE DELITOS INFORMATICOS

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**, cometidos mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia.

CAPITULO II
DELITOS CONTRA DATOS Y SISTEMAS INFORMÁTICOS

Artículo 2. Acceso ilícito

El que **accede sin autorización a todo o en parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo**, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.

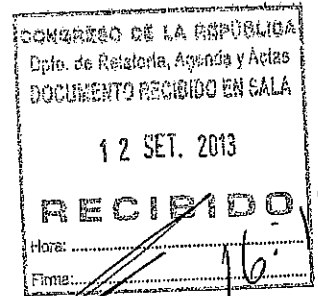
Será reprimido con la misma pena, el que **accede a un sistema informático excediendo lo autorizado**.

Artículo 3. Atentado a la integridad de datos informáticos

El que, a través de las tecnologías de la información o de la comunicación, **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, a través de las tecnologías de la información o de la comunicación, **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. Propositiones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos

El que, a través de las tecnologías de la información o de la comunicación, contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con una pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal.

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 e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal.

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

Artículo 6. Tráfico ilegal de datos

El que, crea, ingresa, o utiliza indebidamente una base de datos sobre una persona natural o jurídica, identificada o identificable, para comercializar, traficar, vender, promover, favorecer o facilitar información relativa a cualquier ámbito de la esfera personal, familiar, patrimonial, laboral, financiera u otro de naturaleza análoga, creando o no perjuicio, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.

Artículo 7. Interceptación de datos informáticos

El que, a través de las tecnologías de la información o de la comunicación, intercepta datos informáticos en transmisiones no públicas, dirigidas a un sistema informático, originadas en un sistema informático o efectuadas 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 las normas de la materia.

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



CAPÍTULO V DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO

Artículo 8. Fraude informático

El que, a través de las tecnologías de la información o de la comunicación, procura para sí o para otro un provecho ilícito en perjuicio de tercero, mediante el **diseño**, introducción, alteración, borrado, supresión, **clonación** de datos informáticos o cualquier interferencia o **manipulación** en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de **tres** 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.

CAPÍTULO VI DELITOS INFORMÁTICOS CONTRA LA FE PÚBLICA

Artículo 9. Suplantación de identidad

El que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.

CAPÍTULO VII DISPOSICIONES COMUNES

Artículo 10. Abuso de mecanismos y dispositivos informáticos

El que 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, seguridad y soberanía nacionales.

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, debe contar 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, podrá 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, con prescindencia de si los mismos están vinculados a una organización criminal, de conformidad con el artículo 341 del Código Procesal Penal, aprobado mediante Decreto Legislativo 957.

TERCERA. Coordinación interinstitucional de la Policía Nacional con el Ministerio Público

La Policía Nacional del Perú fortalece al 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 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.

CUARTA. Cooperación operativa

Con el objeto de garantizar el intercambio de información, equipos de investigación conjuntos, transmisión de documentos, interceptación de comunicaciones, y demás actividades correspondientes para dar efectividad a la presente Ley, la Policía Nacional del Perú, el Ministerio Público, Poder Judicial y los operadores del sector privado involucrados en la lucha contra los delitos informáticos deben establecer protocolos de



cooperación operativa reforzada 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 Informático (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.

SÉPTIMA. Buenas prácticas

El Estado peruano realizará 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 establecerá los mecanismos de prevención necesarios, incluyendo respuestas coordinadas e intercambio de información y buenas prácticas.

OCTAVA. Convenios multilaterales

El Estado peruano promoverá 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 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 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.

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 Decreto Legislativo 991, en los siguientes términos:

“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.

Sólo 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
Modificase 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.

(...).”

TERCERA. Modificación del Código Procesal Penal

Modificase 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, en los siguientes términos:

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

(...)

4. Los concesionarios de servicios públicos de telecomunicaciones deben 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 guardar secreto acerca de las mismas, salvo que se le citare como testigo 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.

(...).”



“Artículo 235. Levantamiento del secreto bancario
(...)”

5. Las empresas o entidades requeridas con la orden judicial deben 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;

(...)”

CUARTA. Modificación de los artículos 162, 183-A y 323 del Código Penal
Modifíquense los artículos 162, 183-A y 323 del Código Penal, aprobado por 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, seguridad o soberanía nacionales.”

“Artículo 183-A. Pornografía infantil

El que posee, promueve, fabrica, distribuye, exhibe, ofrece, comercializa o pública, 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.”

“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.

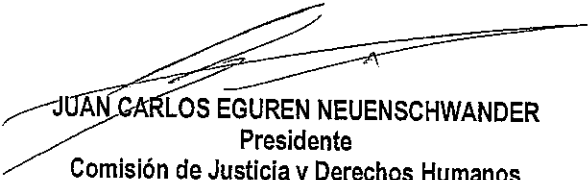
Si el agente es funcionario o servidor público la pena será no menor de dos, ni mayor de cuatro años e inhabilitación conforme al numeral 2 del artículo 36.

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.”

DISPOSICIÓN COMPLEMENTARIA DEROGATORIA

ÚNICA. Derogatoria

Deróganse el numeral 3 del segundo párrafo del artículo 186, y los artículos 207-A, 207-B, 207-C y 207-D del Código Penal.


JUAN CARLOS EGUREN NEUENSCHWANDER
Presidente

Comisión de Justicia y Derechos Humanos
Congreso de la República

1. The first part of the document discusses the importance of maintaining accurate records of all transactions and activities. It emphasizes that this is crucial for ensuring transparency and accountability in the organization's operations.

2. The second part of the document outlines the specific procedures and protocols that must be followed to ensure that all records are properly maintained and updated. It details the roles and responsibilities of the staff involved in this process.