

LEGISLACIÓN INFORMÁTICA

Unidad IV: La Legislación y Normatividad Actual Relativa a la Información



INSTITUTO TECNOLÓGICO
DE MORELIA

Departamento de Sistemas y
Computación

Disponible en: www.benito.org.mx

M.C. Benito Sánchez Raya
sanchezraya@hotmail.com

CONTENIDO

1. Casos de normatividad aplicada a la información.
 - a) Daños a datos
 - b) Robos de datos
 - c) Acceso no autorizado a datos
2. Debilidades o Insuficiencias de la Normatividad
 - a) Amenazas informáticas
 - b) El derecho de la sociedad a la Información

1. CASOS DE NORMATIVIDAD APLICADA A LA INFORMACIÓN

- **DAÑOS A DATOS**

- Definiciones de datos:

(Establecidas en la minuta proyecto de decreto para expedir la Ley Federal de Protección de Datos Personales, presentada al Senado en 2002. No promulgada)

- **Artículo 4.**

- 1. Para los efectos de esta ley se entiende por:

- **I. Datos personales:** La información de la persona física determinada o determinable;

- **II. Datos sensibles:** Aquellos que revelan el origen racial, étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical, salud o vida sexual;
- **III. Archivo, registro, base o banco de datos:** Conjunto de datos personales organizados, tratados automatizadamente;
- **IV. Tratamiento de datos:** Operaciones y procedimientos sistemáticos que tienen por objeto recolectar, guardar, ordenar, modificar, relacionar, cancelar y cualquiera otra que implique el procesamiento de datos, o su cesión a terceros a través de comunicaciones, consultas, interconexiones y transferencias;

- **V. Responsable del archivo, registro, base o banco de datos:** Persona física o jurídica que ostenta la titularidad del archivo, registro, banco o base de datos;
- **VI. Usuario de datos:** Toda persona física, jurídica, pública o privada que trata datos personales de manera voluntaria, ya sea en archivos, registros, bancos de datos propios o a través de conexión con los mismos;
- **VII. Disociación de datos:** Todo tratamiento de datos personales que impida asociarlos a persona determinada o determinable; y,
- **VIII. Interesado:** La persona física a la que conciernen los datos personales.

- Entenderemos por daños a datos, la alteración o modificación, destrucción o pérdida, sin consentimiento y de mala fe, a la estructura lógica o de contenido de dicho dato.

- En México esta tipificado daño a la información.

Código Penal Federal:

TITULO NOVENO

Revelación de secretos y acceso ilícito a sistemas
y equipos de informática

Capítulo II

Acceso ilícito a sistemas y equipos de informática

Artículos 211 bis 1 a bis 7.

– Código Penal Federal:

- **Artículo 211 bis 1.-** Al que sin autorización **modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos** por algún mecanismo de seguridad, se le impondrán de **seis meses a dos años de prisión y de cien a trescientos días multa.**

Al que sin autorización **conozca o copie información contenida en sistemas o equipos de informática protegidos** por algún mecanismo de seguridad, se le impondrán de **tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.**

- **Artículo 211 bis 2.-** Al que sin autorización **modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad,** se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

Al que sin autorización **conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad,** se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

- **Artículo 211 bis 3.-** Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.
- Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

- **Artículo 211 bis 4.-** Al que sin autorización **modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad,** se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.
Al que sin autorización **conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad,** se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

- **Artículo 211 bis 5.-** Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.
- Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.
- Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

- **Artículo 211 bis 6.-** Para los efectos de los artículos 211 Bis 4 y 211 Bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este Código.
- **Artículo 211 bis 7.-** Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

● ROBOS DE DATOS

- El robo de datos es una práctica muy común.
- Se realiza con mayor frecuencia por parte del personal dentro de las propias instituciones o empresas.
- Estas acciones conllevan a una de las grandes pérdidas del capital más importante: *La Información.*

- En el Código Penal Federal en su Título Noveno Capítulo I, II en el Artículo 211 se hace referencia y se estipulan las sanciones relacionadas a acciones como la obtención de datos de forma ilícita.
 - El Capítulo II, Artículos 211 bis 1 al bis 7, ya se analizaron anteriormente.
 - Por lo que solo se detalla el Capítulo I.



Código Penal Federal:

TITULO NOVENO

Revelación de secretos y acceso ilícito a
sistemas
y equipos de informática

Capítulo I

Revelación de secretos

Artículos 210, 211 y 211 Bis

- **Artículo 210.-** Se impondrán de treinta a doscientas jornadas de trabajo en favor de la comunidad, al que sin justa causa, con perjuicio de alguien y sin consentimiento del que pueda resultar perjudicado, **revele algún secreto o comunicación** reservada que conoce o ha recibido con motivo de su empleo, cargo o puesto.
- **Artículo 211.-** La sanción será de uno a cinco años, multa de cincuenta a quinientos pesos y suspensión de profesión en su caso, de dos meses a un año, **cuando la revelación punible sea hecha por persona que presta servicios profesionales o técnicos o por funcionario** o empleado público o cuando el secreto revelado o publicado sea de carácter industrial.

- **Artículo 211 Bis.-** A quien revele, divulgue o utilice indebidamente o en perjuicio de otro, **información o imágenes** obtenidas en una intervención de comunicación privada, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa.
- *¿Podría entrar el messenger y Mail?*

● ACCESO NO AUTORIZADO A DATOS

- Se le adjudica generalmente a los “*hackers*”.
- Estas acciones dependen en su mayoría por el usuario o empleado disgustado o mal intencionado, perteneciente a la institución.
- En el Código Penal Federal en su Título Noveno Capítulo II en los artículos 211 **no se hace una clara referencia.**
- Sin embargo, se estipulan las sanciones relacionadas a acciones consecuentes de no tener una autorización para realizar ciertas actividades.

- Desde Abril del 2004 la Cámara de Diputados aprobó un proyecto de reforma penal para castigar hasta con dos años de cárcel a los llamados “*hackers*” o piratas cibernéticos que se introduzcan en sistemas de cómputo para realizar fraudes, sustraer información, bancos de datos o infectar sistemas.
- Los llamados hackers serán considerados como delincuentes de la informática, según lo establecen las reformas al artículo 211 bis 1; 211 bis 8 y 211 bis 9 del Código Penal Federal y se les impondrá sanción de seis meses a dos años de prisión y de 100 a 300 días multa.

– Sin embargo este proyecto de reforma no ha fructificado, la última vez que ha sido desechado fue el 4 de Diciembre de 2007.

– Proyecto completo:

<http://www.senado.gob.mx/gace2.php?sesion=2004/04/22/1&documento=19>

– Desechado:

http://archivos.diputados.gob.mx/servicios/datorele/LX_LEG/1%20POS%20II%20ANO/04-dic-07/9b.htm

● Artículos del proyecto relacionados con acceso no autorizado a datos:

- **Artículo 211 BIS 6.-** Al que **sin autorización o excediendo la que hubiere obtenido acceda a la totalidad o parte de un sistema informático** o equipo informático se le impondrá una pena de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.
- Cuando se acceda a sistemas informáticos o equipos informáticos protegidos por algún mecanismo de seguridad, o a sistemas o equipos informáticos del Estado o de las instituciones que integran el sistema financiero, la pena a que se refiere el párrafo anterior se aumentará en una mitad.

- **Artículo 211 BIS 7.-** Al que sin autorización intercepte por medios técnicos, datos informáticos comunicados en transmisiones no públicas efectuadas en un sistema informático, desde un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos informáticos se le impondrá una pena de dos a cuatro años de prisión y de trescientos a seiscientos días multa.

● PANORAMA LEGAL A NIVEL MUNDIAL

- **Alemania:** Sancionó en **1986** la Ley contra la Criminalidad Económica que contempla los siguientes delitos, espionaje de datos, alteración de datos entre otros.
- **Francia:** En Enero de **1988**, este país dictó la Ley Relativa al Fraude Informático, la cual prevé penas de dos meses hasta dos años de prisión y multas de diez mil a cien mil francos por la intromisión fraudulenta que suprima o modifique datos.

- **Austria:** Ley de reforma del Código Penal, promulgada en Diciembre de **1987**, sanciona aquellos que con dolo causen un perjuicio patrimonial, a un tercero influyendo en el resultado de la elaboración automática de datos a través de la confección de del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos. Además contempla sanciones para quienes cometen este hecho utilizando su profesión de especialistas en sistemas.

- **España:** El Artículo 264-2, del Código Penal de España, establece que se aplicará la pena de prisión de uno a tres años y multa a quien por cualquier medio destruya, altere o inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

2. DEBILIDADES O INSUFICIENCIAS DE LA NORMATIVIDAD

- Gran parte de las insuficiencias de la legislación actual se deben a:
 - El retraso que se presenta en la aprobación de proyectos de reformas y leyes sobre delitos informáticos.
 - Cada vez se vuelven más recurrentes dichos delitos.
 - El desconocimiento de los diferentes tipos de delincuencia informática.
 - Su pobre penalización.

● AMENAZAS INFORMÁTICAS

- Son programas hechos con la finalidad de instalarse y reproducirse.
- Fuente principal de contagio: Internet
 - Mails, chat, mensajería instantánea, medios extraíbles, etc
- Los virus es solo un tipo mas de amenaza.
- Los virus se pueden clasificar:
 - Según su origen, las técnicas que utilizan para infectar, los tipos de archivos que infectan, los lugares donde se esconden, los daños que causan, el sistema operativo o la plataforma tecnológica que atacan, entre otros.

- **Residentes:** Se ocultan en la memoria RAM de forma permanente o residente. Controlan e interceptan todas las operaciones llevadas a cabo por el sistema operativo, infectando todos aquellos archivos que sean ejecutados, abiertos, cerrados, renombrados, copiados, etc.
- **De acción directa:** Su objetivo es reproducirse y actuar al momento de ser ejecutado. Al cumplirse una determinada condición, se activan y buscan los archivos para contagiarlos.

- **De sobre escritura:** Destruyen la información contenida en los archivos que infectan. Cuando infectan un archivo, escriben dentro de su contenido, haciendo que queden total o parcialmente inservible.
- **De Boot:** Dañan el sector de arranque de discos duros o memorias extraíbles.
- **De macro:** Infectan los archivos creados con determinadas aplicaciones que contengan macros: como los archivos de MSOffice, entre otros.

- **Multipartites:** Virus avanzados, pueden realizar múltiples infecciones, combinando diferentes técnicas para ello. Su objetivo: cualquier elemento que pueda ser infectado: archivos, programas, macros, discos, etc.
- **De fichero (archivo):** Infectan programas o archivos ejecutables. Al ejecutarse el programa infectado, el virus se activa, produciendo diferentes efectos.

- **De compañía:** Son virus de archivo que al mismo tiempo pueden ser residentes o de acción directa. Acompañan a otros archivos existentes en el sistema antes de su llegada, sin modificarlos.
- **De FAT:** Los virus que atacan a este elemento son peligrosos, impedirán el acceso a ciertas partes del disco, donde se almacenan los archivos críticos. Los daños causados a la FAT se traducirán en pérdidas de la información contenida en archivos individuales y en directorios completos.

- **Cifrados:** Se cifran a sí mismos para no ser detectados. Para realizar sus actividades, el virus se descifra a sí mismo y, cuando ha finalizado, se vuelve a cifrar.
- **Polifórmicos:** En cada infección que realizan se cifran de una forma distinta.
- **De enlace o directorio:** Alteran las direcciones que indican donde se almacenan los archivos. Al intentar ejecutar un programa, lo que se hace en realidad es ejecutar el virus, éste habrá modificado la dirección donde se encontraba originalmente el programa, colocándose en su lugar.

- **Gusanos:** Realizan copias de sí mismos a la máxima velocidad posible, sin tocar ni dañar archivos. Sin embargo, se reproducen con gran rapidez que pueden colapsar por saturación las redes o sistemas, en donde se infiltran.
- **Troyanos:** Técnicamente, no se consideran virus. Su objetivo básico es la introducción e instalación de otros programas en la computadora, para permitir su control remoto desde otros equipos.

- **Bombas lógicas:** Destruyen los datos de una computadora o causan otros daño de consideración en ella, cuando se cumplen ciertas condiciones. Mientras este hecho no ocurra, nadie se percata de su presencia.

Legislación sobre amenazas Informáticas

- La **Ley Federal del Derecho de Autor** regula todo lo relativo a la protección de los programas de computación, a las bases de datos y a los derechos autorales relacionados con ambos.

- En ella se define lo que es un programa de computación, su protección, sus derechos patrimoniales, de arrendamiento, casos en los que se podrá realizar copias del programa, las facultades de autorizar o prohibir la reproducción, la autorización del acceso a la información de carácter privado relativa a las personas contenida en las bases de datos, la publicación, reproducción, divulgación, comunicación pública y transmisión de dicha información, establece las infracciones y sanciones que deben ser aplicadas cuando ocurren ilícitos relacionados con lo anterior.

Ley Federal del Derecho de Autor

TITULO IV

De la Protección al Derecho de Autor

Capítulo IV

De los Programas de Computación y las Bases de Datos

- **Artículo 101.-** Se entiende por programa de computación la expresión original en cualquier forma, lenguaje o código, de un conjunto de instrucciones que, con una secuencia, estructura y organización determinada, tiene como propósito que una computadora o dispositivo realice una tarea o función específica.

- **Artículo 102.-** Los programas de computación se protegen en los mismos términos que las obras literarias. Dicha protección se extiende tanto a los programas operativos como a los programas aplicativos, ya sea en forma de código fuente o de código objeto. **Se exceptúan aquellos programas de cómputo que tengan por objeto causar efectos nocivos a otros programas o equipos.**

Ley Federal del Derecho de Autor
TITULO XII
De los Procedimientos Administrativos
Capítulo II
De las Infracciones en Materia de Comercio

- **Artículo 231.-** Constituyen infracciones en materia de comercio las siguientes conductas cuando sean realizadas con fines de lucro directo o indirecto:

- I.
- II.
- III.
- IV.
- V. Importar, vender, arrendar o realizar cualquier acto que permita tener un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación;
- VI.
- Etc.

- **Artículo 232.-** Las infracciones en materia de comercio previstos en la presente Ley serán sancionados por el Instituto Mexicano de la Propiedad Industrial con multa:
 - I. De cinco mil hasta diez mil días de salario mínimo en los casos previstos en las fracciones I, III, IV, **V**, VII, VIII y IX del artículo anterior;

● **EL DERECHO DE LA SOCIEDAD A LA INFORMACIÓN**

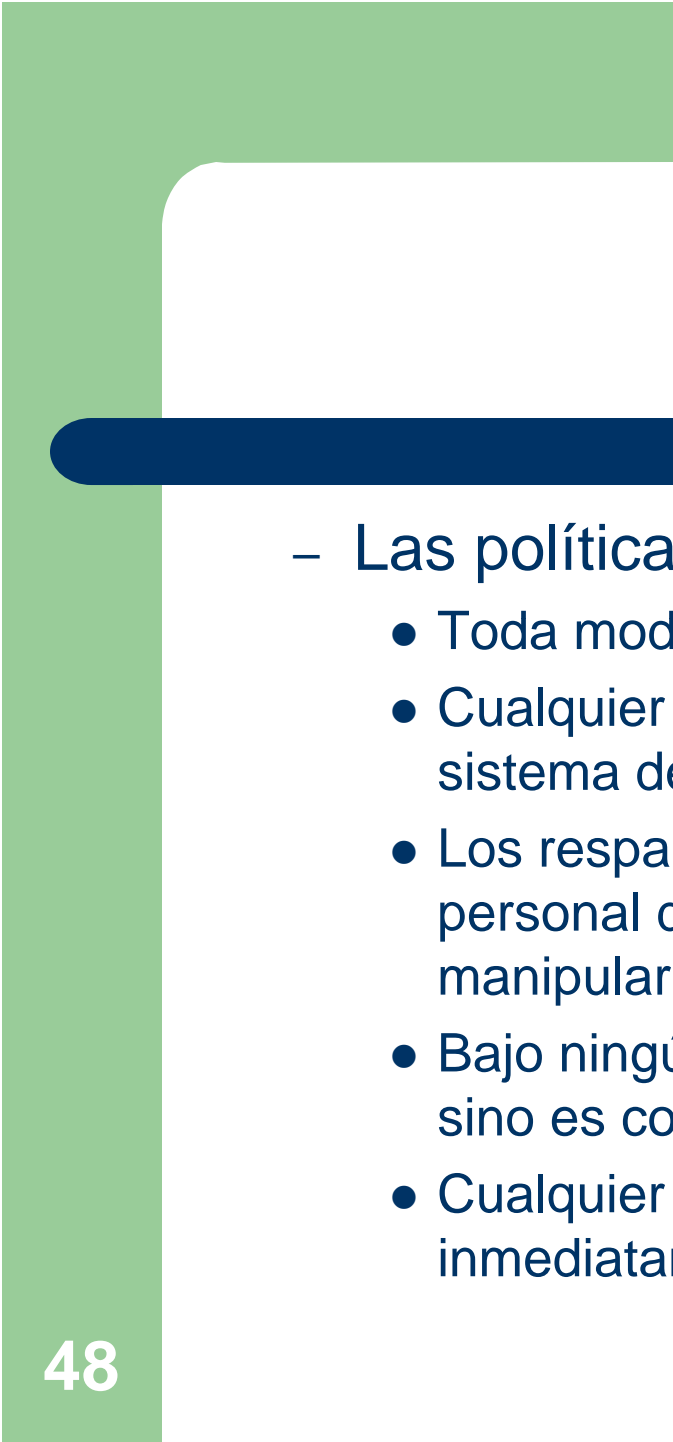

- La información representa un importante y creciente recurso para la potenciación política, social y económica.
- Las nuevas TICs pueden llegar a vulnerar algunos derechos humanos como el derecho a la privacidad y el derecho a la intimidad.
- Actualmente se trabaja en el diseño y la implementación de políticas públicas centradas en los Derechos Humanos.
- Lo anterior debido a que la Sociedad de la Información es una sociedad en formación.

- La relación entre la Sociedad de la Información y los Derechos Humanos deberá estar fundamentada en el respeto a la dignidad humana
- Principio universal contenido en el **Artículo 12 de la Declaración Universal de los Derechos Humanos**.
- Se menciona que nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, asimismo en su honra o su reputación, teniendo el derecho a la protección de la ley contra tales injerencias.

- Ésta declaración fue adoptada y proclamada por la Resolución de la Asamblea General 217 A (III) del 10 de Diciembre de 1948, por la ONU.
 - <http://www.un.org/spanish/aboutun/hrights.htm>
- **Artículo 12.-** Nadie será objeto de injerencias arbitrarias a su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias y ataques.

- La nueva Sociedad de la Información deberá comprender un nuevo orden económico internacional, una mejor relación entre la humanidad y el planeta, incluido el respeto al medio ambiente y las políticas ecológicas y en general todo aquello que evite que el productivismo tecnocientífico continúe imponiendo su lógica destructiva e irresponsable para el futuro del planeta y de la especie humana.

- **Caso sociedad cooperativa de ahorro y prestamos monetarios, Morelia, Michoacán.**
 - Dentro de la estructura organizacional de esta empresa, se encuentra la Gerencia de Tecnologías, en ella se trabaja con una serie de políticas y normas que le permiten asegurar las operaciones relacionadas con la **Seguridad de los Datos.**

- 
- 
- Las políticas a las que haremos referencia son:
 - Toda modificación al sistema debe estar amparada.
 - Cualquier solicitud de información no contenida en el sistema deberá ser pedida a través del formato.
 - Los respaldos se deberán resguardar en caja fuerte y solo personal de base de datos tendrá la autoridad para manipularlos.
 - Bajo ningún motivo se realizará la modificación de datos sino es con el respaldo del escrito autorizado.
 - Cualquier falla en el equipo de cómputo debe reportarse inmediatamente.

- El usuario es responsable de resguardar su información (creación, modificación y eliminación de archivos).
- El usuario es responsable de cualquier mal uso, pérdida o robo del equipo que tenga asignado.
- Por ningún motivo cualquier equipo de cómputo podrá ser extraído del lugar de trabajo, solo bajo solicitud por escrito del responsable del mismo y con autorización de la Gerencia de Tecnologías de la Información. Incluyendo los equipos portátiles.
- Es responsabilidad del usuario tener su equipo de computo libre de objetos así como el de tenerlo limpio.

- El responsable del equipo de cómputo debe respetar la configuración que tenga el equipo al momento de la asignación y no modificar el hardware y software del equipo de cómputo bajo ninguna circunstancia.
- Las sanciones serán de acuerdo a la gravedad de la falta y/o cantidad de reincidencias a la misma. Y van desde la llamada de atención verbal hasta un acta administrativa.

● **ACTIVIDADES DE APRENDIZAJE**

– Leer y discutir:

- Ley Federal de Protección de Datos Personales, Proyecto 2002.
- Reformas en Materia de Delitos Informáticos, propuestas por el Senado Mexicano, desde 2004.
- Declaración universal de los derechos humanos de la ONU.



- **REFERENCIAS**

Material de Titulación

Arturo García Velázquez. 2006.

Instituto Tecnológico de Morelia.