**CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS**

**Artículo 6° Constitucional**

**Derecho de acceso a la información pública y protección de datos personales**

Este artículo establece que:

* **Toda la información en posesión de cualquier autoridad, entidad, órgano o dependencia gubernamental es pública**, y solo puede ser reservada temporalmente por razones de **interés público y seguridad nacional**.
* **El Estado garantizará el derecho de acceso a la información.**
* También se reconoce el **derecho a la protección de datos personales**, el cual implica que toda persona tiene control sobre sus datos y puede **acceder, rectificar, cancelar u oponerse (ARCO)** al uso de los mismos.
* Se establece que debe existir un **organismo autónomo especializado, imparcial y colegiado** que garantice ambos derechos: acceso a la información y protección de datos personales (en la práctica, es el **INAI**: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales).

**Fragmento clave**:

*"Toda persona tiene derecho al acceso a la información y a la protección de sus datos personales, en los términos que fijen las leyes."*

**Artículo 16° Constitucional**

**Derecho a la privacidad y protección frente al uso indebido de información personal**

Este artículo protege la **vida privada y los datos personales** de los ciudadanos, e indica que:

* **Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones** sino por mandato escrito de autoridad competente y justificado legalmente.
* **Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición.**
* La ley establecerá las bases y condiciones para el tratamiento de los datos personales, garantizando su protección.

**Fragmento clave**:

*"Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición..."*

**LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES (LFPDPPP)**

**Artículo 3 – Definiciones y principios fundamentales**

Este artículo **define conceptos clave** y **establece los principios rectores** del tratamiento de datos personales. Algunos puntos esenciales son:

**Definiciones importantes:**

* **Datos personales**: Cualquier información concerniente a una persona física identificada o identificable.
* **Datos personales sensibles**: Aquellos que afectan la esfera más íntima del titular, como origen étnico, estado de salud, creencias religiosas, opiniones políticas, orientación sexual, etc.
* **Responsable**: Persona física o moral que decide sobre el tratamiento de los datos.
* **Encargado**: Persona física o moral que trata datos por cuenta del responsable.

**Principios que rigen el tratamiento de datos:**

1. **Licitud**: El tratamiento debe hacerse conforme a la ley.
2. **Consentimiento**: El titular debe autorizar el tratamiento de sus datos.
3. **Información**: El titular debe ser informado sobre cómo se usan sus datos (a través del aviso de privacidad).
4. **Calidad**: Los datos deben ser exactos y actualizados.
5. **Finalidad**: Solo pueden usarse para los fines legítimos que se informaron.
6. **Lealtad**: El tratamiento debe hacerse sin engaños.
7. **Proporcionalidad**: Solo deben recabarse los datos necesarios.
8. **Responsabilidad**: El responsable debe garantizar y demostrar el cumplimiento de estos principios.

**Artículo 8 – Consentimiento para el tratamiento de datos (especialmente en menores)**

Este artículo establece que:

* El **tratamiento de datos personales requiere el consentimiento del titular**, salvo excepciones previstas en la ley (por ejemplo, cuando es necesario para cumplir una obligación legal o por razones de seguridad pública).
* **Debe informarse al titular con claridad para qué fines se usarán sus datos.**
* El consentimiento puede ser **expreso o tácito**, dependiendo del tipo de datos.

**Tratamiento de datos de menores de edad:**

* Aunque la LFPDPPP **no especifica una edad mínima**, se interpreta conjuntamente con la **Ley General de los Derechos de Niñas, Niños y Adolescentes (LGDNNA)**, la cual establece que:
  + A partir de los **13 años**, los adolescentes pueden **dar su consentimiento para el tratamiento de sus datos personales**, siempre que se les informe de forma clara, accesible y adecuada a su edad y madurez.
  + Si son **menores de 13 años**, el **consentimiento debe ser otorgado por sus padres, tutores o representantes legales.**

**LEY GENERAL DE LOS DERECHOS DE NIÑAS, NIÑOS Y ADOLESCENTES (LGDNNA)**

**Artículo 76 – Derecho a la protección de la vida privada y los datos personales en entornos digitales**

Este artículo reconoce explícitamente que:

* **Niñas, niños y adolescentes tienen derecho a la protección de su vida privada y de sus datos personales**, especialmente en el entorno digital.
* Toda persona o institución que trate datos personales de menores **debe garantizar su privacidad**, asegurando el respeto a su **dignidad e integridad personal**.
* Se deben considerar factores como:
  + Edad del menor
  + Capacidad de discernimiento
  + Evolución de sus facultades

**Esto implica** que cualquier aplicación, red social, servicio educativo o plataforma digital debe adoptar **medidas especiales de protección de datos** cuando el usuario es menor de 18 años.

**Obligaciones derivadas:**

* Solicitar consentimiento informado de forma clara y accesible.
* Evitar la recolección excesiva de datos.
* No utilizar sus datos para fines no autorizados.
* Establecer **mecanismos de control parental cuando sea pertinente.**

**Artículo 77 – Promoción de la educación en seguridad digital**

Este artículo establece que:

* El **Estado debe promover políticas públicas y programas educativos** que **formen a niñas, niños y adolescentes en el uso seguro, responsable y crítico de las tecnologías digitales**.
* La educación digital debe:
  + Protegerlos frente a **riesgos como el ciberacoso, grooming, sexting, fraudes, robo de identidad, etc.**
  + Fortalecer su conocimiento sobre **privacidad, reputación digital, huella digital y protección de datos personales.**
  + Impulsar su **participación segura y activa en entornos digitales.**

**Esto implica** que es una **obligación legal del Estado** (y también una responsabilidad compartida por instituciones educativas y desarrolladores de tecnología) ofrecer herramientas y formación para que los menores comprendan y **ejerciten sus derechos digitales**.

**Ley Federal de Ciberseguridad y Confianza Digital**

**Artículo 2 – Objetivos de la Ley**

Este artículo define los **objetivos generales** de la Ley Federal de Ciberseguridad y Confianza Digital, entre los que se destacan:

* **Fomentar la cultura de la ciberseguridad entre la población**, con enfoque preventivo y formativo.
* Promover **la protección de datos personales** en los entornos digitales.
* Impulsar acciones de **educación digital**, principalmente en sectores vulnerables como **niñas, niños y adolescentes**.
* Establecer medidas para **prevenir y mitigar riesgos en el ciberespacio**, incluyendo delitos informáticos, fraudes, robo de identidad y más.

**Esto significa que educar adolescentes sobre cómo proteger sus datos y actuar con responsabilidad digital no solo es importante, sino un objetivo legal respaldado por el Estado mexicano.**

**Artículo 3 – Principios rectores**

Este artículo establece los **principios bajo los cuales debe implementarse la ley**, y que deben guiar todas las acciones públicas y privadas en materia de ciberseguridad:

1. **Inclusión digital**: Todas las personas, sin importar su nivel socioeconómico o lugar de residencia, deben tener acceso a herramientas y educación en ciberseguridad.
2. **No discriminación**: La ley protege a grupos en situación de vulnerabilidad, como niñas, niños y adolescentes, para que tengan **igualdad de condiciones en el entorno digital**.
3. **Seguridad digital**: Todas las actividades en línea deben desarrollarse en condiciones de seguridad y confianza, protegiendo la **integridad de los datos** y la identidad digital de las personas.

Estos principios refuerzan la **obligación ética y legal** de desarrollar soluciones digitales **inclusivas, seguras y accesibles** para adolescentes, garantizando su derecho a un entorno digital protegido.

**Artículo 25 – Funciones del INFOTEC**

Este artículo asigna funciones específicas al **INFOTEC (Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación)**, destacando las siguientes:

* Desarrollar **programas de capacitación, educación y sensibilización en materia de ciberseguridad**, enfocados en toda la población, pero con **especial atención a menores de edad**.
* Apoyar el diseño de **materiales formativos**, talleres, campañas digitales y herramientas tecnológicas para la prevención de riesgos cibernéticos.
* Promover la **alfabetización digital desde edades tempranas**, y colaborar con instituciones educativas y organizaciones sociales.

Esto convierte al INFOTEC en un **aliado institucional clave** para iniciativas educativas en ciberseguridad enfocadas en adolescentes.