

Clase 11 — Derecho Informático, Internet y Gobierno Electrónico

Tecnicatura Universitaria en Programación — UTN

Duración total: 120 minutos

Objetivos de la clase

Al finalizar la clase, el estudiante deberá poder:

- Comprender el concepto y alcance del Derecho Informático.
 - Identificar las principales problemáticas jurídicas derivadas del uso de tecnologías digitales.
 - Reconocer la estructura institucional y normativa de internet.
 - Analizar críticamente principios como neutralidad de la red y gobernanza digital.
 - Comprender el funcionamiento jurídico del gobierno electrónico en Argentina.
 - Relacionar el Derecho Informático con la protección de datos personales y los derechos fundamentales.
-

¿Qué es el Derecho Informático?

Primera aproximación conceptual

El Derecho Informático es la disciplina jurídica que estudia, regula y analiza los efectos legales producidos por el uso de tecnologías de la información y la comunicación (TICs), especialmente

cuando dichas tecnologías impactan sobre derechos, obligaciones, responsabilidades y relaciones sociales.

Se trata de una rama jurídica dinámica y transversal, porque la tecnología atraviesa prácticamente todas las actividades humanas contemporáneas:

- comunicación,
- comercio,
- administración pública,
- educación,
- salud,
- trabajo,
- finanzas,
- entretenimiento,
- inteligencia artificial,
- redes sociales,
- almacenamiento de datos.

En consecuencia, el Derecho Informático surge como respuesta a una necesidad concreta: adaptar el sistema jurídico tradicional a una realidad digital en constante evolución.

Definición técnica

Puede definirse al Derecho Informático como:

“La disciplina jurídica que regula las relaciones derivadas de la creación, uso, tratamiento, transmisión y almacenamiento de información mediante sistemas tecnológicos.”

Tres grandes ejes del Derecho Informático

1. Los efectos jurídicos derivados del uso de tecnologías

Toda interacción tecnológica puede producir consecuencias legales.

Ejemplos cotidianos

- aceptar términos y condiciones en una app,
- realizar una compra online,
- utilizar firma digital,
- almacenar datos en la nube,
- publicar contenido en redes sociales,
- utilizar inteligencia artificial,
- enviar un correo electrónico laboral.

Cada una de estas acciones puede generar:

- contratos,
 - obligaciones,
 - responsabilidad civil,
 - delitos,
 - protección de derechos,
 - conflictos de jurisdicción,
 - problemas de privacidad.
-

Ejemplo práctico

Cuando una persona acepta los “Términos y Condiciones” de una plataforma como Mercado Libre o Meta:

- existe consentimiento jurídico,
- se perfecciona un contrato electrónico,
- nacen obligaciones para ambas partes.

Aunque el usuario muchas veces no lea el texto completo, jurídicamente el acto tiene efectos válidos.

2. El tratamiento automatizado de información

Uno de los núcleos centrales del Derecho Informático es la regulación de los datos.

La sociedad digital funciona a partir de información procesada automáticamente por sistemas informáticos.

¿Qué significa “tratamiento automatizado”?

Es cualquier operación realizada sobre datos mediante sistemas tecnológicos.

Puede incluir:

- recolección,
 - almacenamiento,
 - clasificación,
 - análisis,
 - transferencia,
 - modificación,
 - eliminación,
 - perfilado algorítmico.
-

Ejemplos actuales

Plataformas digitales

Google analiza búsquedas.

Netflix recomienda contenidos mediante algoritmos.

TikTok perfila usuarios según comportamiento.

Problemas jurídicos que aparecen

Privacidad

¿Quién puede usar nuestros datos?

Consentimiento

¿El usuario realmente comprende qué autoriza?

Seguridad informática

¿Qué ocurre si hay una filtración?

Discriminación algorítmica

¿Puede un algoritmo tomar decisiones injustas?

Transferencia internacional de datos

¿Qué sucede cuando los servidores están en otro país?

Protección de datos personales

En Argentina, la materia se encuentra regulada principalmente por:

Ley 25.326

Esta norma reconoce principios fundamentales como:

- consentimiento informado,
 - finalidad,
 - calidad de datos,
 - confidencialidad,
 - seguridad.
-

3. Las relaciones digitales entre personas, empresas y Estado

El Derecho Informático también regula cómo interactúan los distintos actores dentro del ecosistema digital.

Relaciones entre particulares

Ejemplos

- contratos electrónicos,
 - comercio digital,
 - marketplaces,
 - redes sociales,
 - servicios en la nube,
 - plataformas de streaming.
-

Relaciones empresa–usuario

Las empresas tecnológicas administran enormes volúmenes de información y prestan servicios digitales globales.

Esto genera cuestiones vinculadas con:

- responsabilidad empresarial,
 - cláusulas abusivas,
 - monopolios digitales,
 - publicidad personalizada,
 - derechos del consumidor.
-

Relaciones Estado–ciudadano

El Estado también utiliza tecnología para:

- administrar información,
 - realizar trámites digitales,
 - emitir documentos electrónicos,
 - controlar sistemas tributarios,
 - gestionar expedientes electrónicos.
-

Ejemplos argentinos

- AFIP
 - ANSES
 - TAD
 - expediente judicial electrónico.
-

Características del Derecho Informático

Característica	Explicación
Dinámico	evoluciona constantemente con la tecnología
Transversal	se relaciona con múltiples ramas jurídicas
Global	internet supera fronteras estatales
Técnico	requiere comprensión tecnológica
Preventivo	busca reducir riesgos digitales

Relación con otras ramas del derecho

El Derecho Informático no funciona aislado.

Se vincula con:

Rama	Ejemplo
Derecho Civil	contratos electrónicos
Derecho Penal	ciberdelitos
Derecho Administrativo	gobierno digital
Derecho Constitucional	privacidad y libertad de expresión
Derecho Laboral	control digital del trabajador
Derecho Internacional	transferencias de datos

Importancia actual

El Derecho Informático se volvió esencial porque gran parte de la vida moderna ocurre en entornos digitales.

Hoy los conflictos jurídicos más relevantes incluyen:

- inteligencia artificial,

- ciberseguridad,
 - protección de datos,
 - plataformas digitales,
 - criptomonedas,
 - vigilancia estatal,
 - identidad digital,
 - deepfakes,
 - algoritmos de decisión automática.
-

“Cada vez que usamos tecnología, también estamos entrando en una relación jurídica.”

Aceptar cookies, subir una foto, usar reconocimiento facial o comprar online no son solamente actos tecnológicos: son actos con consecuencias jurídicas concretas.

Concepto y naturaleza del Derecho Informático

1. Definición doctrinaria

Concepto técnico-jurídico

El Derecho Informático puede definirse como:

“El conjunto de normas, principios e instituciones que regulan los efectos jurídicos derivados de la informática y de las tecnologías digitales.”

Esta definición permite comprender que el Derecho Informático no se limita únicamente al uso de computadoras o internet, sino que abarca todas las consecuencias jurídicas producidas por el tratamiento digital de la información y por la utilización de tecnologías en la vida social, económica y estatal.

Análisis de la definición

“Conjunto de normas”

Hace referencia al marco normativo positivo aplicable.

Ejemplos en Argentina:

- Ley 25.326
- Ley 25.506
- Ley 26.388
- Ley 27.078

Estas normas regulan:

- datos personales,
- firma electrónica,
- delitos tecnológicos,
- telecomunicaciones,
- servicios digitales.

“Principios”

El Derecho Informático también se apoya en principios jurídicos generales y específicos.

Ejemplos

- principio de privacidad,
- neutralidad tecnológica,
- neutralidad de la red,
- autodeterminación informativa,

- seguridad informática,
 - consentimiento informado.
-

“Instituciones”

Son las estructuras jurídicas que organizan relaciones digitales.

Ejemplos:

- firma digital,
 - expediente electrónico,
 - contratos electrónicos,
 - identidad digital,
 - habeas data,
 - prueba informática.
-

“Efectos jurídicos derivados de la informática”

La informática produce consecuencias legales concretas.

Por ejemplo:

Acción tecnológica	Consecuencia jurídica
Comprar online	contrato electrónico
Filtrar datos personales	responsabilidad civil

Hackear un sistema	delito penal
Usar firma digital	autenticación jurídica
Publicar contenido difamatorio	daño al honor

Características del Derecho Informático

Dinámico

La tecnología evoluciona constantemente y el derecho debe adaptarse.

Interdisciplinario

Combina:

- derecho,
 - informática,
 - ciberseguridad,
 - telecomunicaciones,
 - protección de datos,
 - inteligencia artificial.
-

Global

Internet trasciende fronteras estatales, lo que genera conflictos de jurisdicción y soberanía.

Preventivo y reactivo

Busca:

- prevenir riesgos tecnológicos,
 - regular conductas digitales,
 - sancionar ilícitos informáticos.
-

2. Naturaleza jurídica

Uno de los debates clásicos dentro de la doctrina consiste en determinar:

si el Derecho Informático constituye una rama autónoma del derecho o si simplemente atraviesa transversalmente las ramas tradicionales.

No existe unanimidad doctrinaria absoluta.

Postura 1 — El Derecho Informático como rama autónoma

Esta postura sostiene que el Derecho Informático posee autonomía científica y jurídica propia.

Fundamentos de esta posición

a) Objeto propio

El Derecho Informático regula fenómenos específicos vinculados con:

- información digital,
 - tecnologías de la información,
 - entornos virtuales,
 - automatización,
 - inteligencia artificial,
 - redes digitales.
-

b) Principios específicos

Posee principios propios que no existían tradicionalmente.

Ejemplos

- autodeterminación informativa,
 - neutralidad de la red,
 - equivalencia funcional,
 - seguridad informática,
 - minimización de datos.
-

c) Metodología diferenciada

El análisis jurídico requiere conocimientos técnicos especializados.

Por ejemplo:

- arquitectura de redes,
- criptografía,
- blockchain,

- algoritmos,
 - ciberseguridad,
 - sistemas de autenticación.
-

d) Problemas jurídicos particulares

Existen conflictos inéditos generados exclusivamente por tecnologías digitales.

Ejemplos característicos

Protección de datos personales

¿Cómo se regula el uso masivo de datos?

Ciberdelitos

¿Cómo se investigan delitos cometidos en entornos digitales?

Firma digital

¿Cómo se acredita identidad en entornos virtuales?

Inteligencia artificial

¿Quién responde por decisiones automatizadas?

Consecuencia doctrinaria

Para esta postura:

el Derecho Informático merece reconocimiento como rama jurídica autónoma, del mismo modo que ocurrió históricamente con el Derecho Laboral o el Derecho Ambiental.

Postura 2 — El Derecho Informático como rama transversal

Otra corriente doctrinaria considera que el Derecho Informático no constituye una rama autónoma.

Según esta visión:

la tecnología simplemente impacta sobre ramas jurídicas preexistentes.

Idea central

El Derecho Informático:

- no reemplaza el Derecho Civil,
- no reemplaza el Derecho Penal,
- no reemplaza el Derecho Administrativo,

sino que introduce nuevas problemáticas dentro de esas ramas tradicionales.

Ejemplos prácticos

Problema digital	Rama aplicable
Contrato online	Derecho Civil y Comercial
Hackeo	Derecho Penal
Protección de datos estatales	Derecho Administrativo
Libertad de expresión en redes	Derecho Constitucional
Teletrabajo	Derecho Laboral
Comercio electrónico internacional	Derecho Internacional Privado

Argumentos de esta postura

a) El derecho sigue siendo el mismo

Cambian los medios tecnológicos, pero no la estructura jurídica básica.

Por ejemplo:

- un contrato digital sigue siendo un contrato,
 - una estafa online sigue siendo una estafa,
 - una injuria en redes sigue siendo una afectación al honor.
-

b) Riesgo de fragmentación excesiva

Crear demasiadas “nuevas ramas” podría generar:

- dispersión normativa,
 - superposición doctrinaria,
 - inseguridad jurídica.
-

c) Dependencia de otras disciplinas

El Derecho Informático depende constantemente de instituciones tradicionales:

- responsabilidad civil,
 - contratos,
 - derechos personalísimos,
 - derecho penal,
 - derecho constitucional.
-

Actualmente, gran parte de la doctrina sostiene una posición intermedia:

el Derecho Informático posee cierta autonomía funcional y temática, pero mantiene una relación transversal con las ramas clásicas del derecho.

Es decir:

- tiene problemas propios,
- desarrolla principios específicos,

- requiere especialización técnica,

pero al mismo tiempo interactúa permanentemente con todo el sistema jurídico.

Importancia práctica del debate

La discusión no es solamente teórica.

Determinar la naturaleza jurídica del Derecho Informático impacta en:

- diseño legislativo,
 - especialización judicial,
 - formación profesional,
 - políticas públicas digitales,
 - regulación de inteligencia artificial,
 - protección de derechos fundamentales en internet.
-

La expansión tecnológica transformó radicalmente la forma en que:

- contratamos,
- trabajamos,
- consumimos,
- nos comunicamos,
- almacenamos información,
- ejercemos derechos.

Por ello, el Derecho Informático surge como una respuesta jurídica necesaria frente a una sociedad cada vez más digitalizada.

La pregunta ya no es si la tecnología influye en el derecho.

La verdadera discusión contemporánea es:

hasta qué punto el derecho puede adaptarse a la velocidad del cambio tecnológico sin perder seguridad jurídica ni protección de derechos fundamentales.

Situación digital	Rama involucrada
Contrato SaaS	Derecho Civil y Comercial
Hackeo	Derecho Penal
Datos biométricos estatales	Derecho Administrativo
Transferencia internacional de datos	Derecho Internacional Privado

3. Fuentes del Derecho Informático

Fuentes tradicionales

Ley

Ejemplos argentinos:

- Ley 25.326 — Protección de Datos Personales
- Ley 25.506 — Firma Digital
- Ley 26.388 — Delitos Informáticos
- Ley 27.078 — Argentina Digital

Jurisprudencia

Los tribunales interpretan:

- privacidad,
 - libertad de expresión online,
 - responsabilidad de plataformas,
 - evidencia digital.
-

Doctrina

Autores relevantes:

- Julio Téllez Valdés
 - Daniel Altmark
 - Pablo Palazzi
 - Lorenzetti (impacto tecnológico y derecho privado)
-

Fuentes técnicas

Normas ISO

Ejemplo:

- ISO 27001 → seguridad de la información.
-

IETF

La Internet Engineering Task Force desarrolla estándares técnicos de internet.

Ejemplo:

- protocolos TCP/IP,
 - RFCs.
-

Usos y costumbres digitales

Ejemplos:

- aceptación mediante click,
 - autenticación en dos pasos,
 - términos y condiciones digitales.
-

4. Relación con otras ramas del derecho

Rama	Relación con el DI
Civil y Comercial	contratos electrónicos
Penal	ciberdelitos
Administrativo	gobierno digital
Constitucional	privacidad y libertad de expresión

Laboral	teletrabajo y monitoreo
Internacional Privado	jurisdicción y datos transfronterizos

Caso de análisis

SaaS (Software as a Service)

Ejemplo:

Una empresa argentina contrata Microsoft 365.

Problemas jurídicos involucrados

- contrato electrónico,
 - protección de datos,
 - jurisdicción internacional,
 - propiedad intelectual,
 - cumplimiento normativo,
 - ciberseguridad.
-

Marco jurídico de internet

1. ¿Qué es internet?

Concepto técnico simplificado

Internet puede definirse como:

“Una red global descentralizada de redes interconectadas que utilizan protocolos comunes de comunicación.”

Descomposición del concepto

“Red global”

Internet funciona a escala mundial.

Permite que dispositivos ubicados en distintos países puedan comunicarse entre sí en tiempo real.

Ejemplo:

- una persona en Argentina puede enviar un correo a Japón en segundos,
 - un servidor en Estados Unidos puede alojar datos de usuarios europeos,
 - una videollamada puede conectar simultáneamente múltiples continentes.
-

“Descentralizada”

Internet no pertenece a un único Estado, empresa o institución.

No existe un “dueño” absoluto de internet.

Su estructura se compone de:

- proveedores de acceso,
- servidores,

- cables submarinos,
- centros de datos,
- organismos técnicos,
- plataformas privadas,
- protocolos compartidos.

Esto tiene enorme relevancia jurídica porque dificulta:

- el control estatal absoluto,
 - la aplicación territorial de leyes,
 - la censura global,
 - la determinación de jurisdicción.
-

“Redes interconectadas”

Internet funciona mediante miles de redes conectadas entre sí.

Por eso se la denomina:

“la red de redes”.

“Protocolos comunes”

La comunicación digital requiere reglas técnicas uniformes.

Los protocolos permiten que sistemas distintos puedan “entenderse”.

Ejemplo:

- TCP/IP,
- HTTP,
- HTTPS,
- DNS.

Sin protocolos comunes, internet no podría funcionar globalmente.

¿Por qué internet importa jurídicamente?

Internet transformó radicalmente la estructura tradicional del derecho.

Antes de internet:

- las relaciones jurídicas estaban vinculadas a territorios físicos,
- las jurisdicciones eran relativamente claras,
- las fronteras estatales delimitaban competencias.

Internet modifica ese esquema.

Principales impactos jurídicos

a) No tiene fronteras físicas

Una conducta digital puede producir efectos simultáneamente en múltiples países.

Ejemplo:

Un contenido publicado en Argentina puede:

- visualizarse en Europa,
 - almacenarse en Estados Unidos,
 - afectar derechos en Brasil.
-

Problema jurídico

¿Qué ley se aplica?

- ¿la del país del usuario?
 - ¿la del servidor?
 - ¿la de la empresa?
 - ¿la del lugar donde se produce el daño?
-

b) Conecta múltiples jurisdicciones

Internet genera conflictos de competencia internacional.

Ejemplo práctico

Una empresa estadounidense recopila datos de usuarios argentinos mediante servidores ubicados en Irlanda.

Posibles jurisdicciones involucradas:

- Argentina,
 - Estados Unidos,
 - Unión Europea.
-

c) Permite circulación masiva de datos

La economía digital funciona mediante flujo constante de información.

Ejemplos:

- redes sociales,
 - nube,
 - inteligencia artificial,
 - plataformas de streaming,
 - comercio electrónico.
-

Problemas jurídicos derivados

Protección de datos personales

¿Quién controla los datos?

Privacidad

¿Hasta dónde pueden monitorear las plataformas?

Ciberseguridad

¿Qué ocurre ante filtraciones masivas?

Vigilancia estatal

¿Puede un gobierno acceder a comunicaciones privadas?

d) Desafía la soberanía estatal tradicional

Los Estados ya no tienen control absoluto sobre el flujo digital dentro de sus fronteras.

Ejemplos

Plataformas globales

Google

Meta

TikTok

operan simultáneamente en decenas de países.

Conflictos frecuentes

- moderación de contenidos,
 - discursos de odio,
 - fake news,
 - censura,
 - protección infantil,
 - tributación digital,
 - monopolios tecnológicos.
-

2. Gobernanza de internet

Concepto

La gobernanza de internet consiste en:

el conjunto de reglas, principios, organismos y mecanismos mediante los cuales se coordina el funcionamiento global de internet.

Internet no posee un “gobierno mundial”.

En cambio, funciona mediante un modelo:

- multisectorial,
- internacional,
- técnico-político.

Participan:

- Estados,
- empresas,
- organismos técnicos,
- universidades,
- sociedad civil.

ICANN

ICANN

Función principal

ICANN administra aspectos esenciales de la infraestructura lógica de internet.

Competencias

a) Nombres de dominio

Gestiona el sistema de dominios.

Ejemplos:

- .com
- .org
- .ar
- .gov

b) Direcciones IP

Coordina la asignación global de direcciones IP.

Las IP permiten identificar dispositivos conectados.

c) Sistema DNS

El DNS traduce nombres comprensibles para humanos en direcciones numéricas.

Ejemplo:

www.google.com → dirección IP correspondiente.

Importancia jurídica

Sin coordinación del DNS:

- internet sería caótica,
 - podrían existir conflictos de nombres,
 - habría inseguridad técnica y comercial.
-

Ejemplos prácticos

¿Quién controla “.com”?

ICANN.

¿Quién administra “.ar”?

En Argentina interviene NIC Argentina bajo regulación estatal.

IETF

Internet Engineering Task Force

Función

La IETF desarrolla estándares técnicos de internet.

Ejemplos

- TCP/IP,
 - protocolos de correo,
 - estándares de seguridad,
 - interoperabilidad de redes.
-

RFCs

La IETF publica documentos llamados RFC (Request for Comments).

Muchos estándares globales surgen allí.

Importancia jurídica indirecta

Aunque la IETF no crea leyes:

- sus estándares impactan sobre privacidad,
 - seguridad,
 - interoperabilidad,
 - protección de datos.
-

IGF

Internet Governance Forum

Función

Espacio internacional de debate sobre políticas digitales.

Fue impulsado por Naciones Unidas.

Participantes

- gobiernos,
 - empresas tecnológicas,
 - universidades,
 - ONGs,
 - especialistas.
-

Temas debatidos

- inteligencia artificial,
 - derechos digitales,
 - ciberseguridad,
 - libertad de expresión,
 - protección de menores,
 - inclusión digital.
-

Característica central

El IGF no dicta normas obligatorias.

Funciona como espacio de diálogo global.

3. Principios fundamentales de internet

Neutralidad de la red

Concepto

La neutralidad de la red implica que:

los proveedores de internet deben tratar de manera igualitaria todo el tráfico de datos.

Consecuencia práctica

No pueden discriminar:

- usuarios,
 - plataformas,
 - aplicaciones,
 - contenidos,
 - servicios.
-

Ejemplo práctico

Un ISP no debería:

- ralentizar Netflix,
 - bloquear WhatsApp,
 - favorecer su propia plataforma de streaming,
 - cobrar por priorizar ciertos contenidos.
-

Fundamentación jurídica

La neutralidad protege:

- libertad de expresión,
 - competencia,
 - innovación,
 - igualdad de acceso.
-

Riesgos de ausencia de neutralidad

Sin neutralidad:

- las grandes empresas podrían comprar prioridad,
 - pequeñas plataformas quedarían relegadas,
 - existiría control indirecto sobre la información.
-

Regulación argentina

La neutralidad de la red se encuentra reconocida en:

Ley 27.078

Libre flujo de información

Concepto

Internet se basa en la libre circulación global de información.

Elementos centrales

Acceso abierto

Cualquier usuario conectado puede acceder a contenidos globales.

Interoperabilidad

Sistemas distintos pueden comunicarse entre sí.

Ejemplo:

- distintos navegadores,
 - distintos sistemas operativos,
 - distintos dispositivos.
-

Circulación global de datos

La información atraviesa fronteras permanentemente.

Importancia jurídica

El libre flujo de información impacta sobre:

- libertad de expresión,
 - acceso al conocimiento,
 - comercio internacional,
 - innovación tecnológica,
 - derechos humanos digitales.
-

Tensiones contemporáneas

El principio de libre circulación entra frecuentemente en conflicto con:

Interés estatal	Ejemplo
Seguridad nacional	bloqueo de plataformas
Protección de datos	restricciones internacionales
Control de contenidos	censura

Tributación digital	regulación de plataformas
---------------------	---------------------------

Caso contemporáneo para debate

Pregunta para estudiantes

“¿Puede un Estado bloquear completamente una red social?”

Variables jurídicas involucradas

- soberanía estatal,
 - libertad de expresión,
 - acceso a la información,
 - seguridad pública,
 - derechos digitales,
 - proporcionalidad de restricciones.
-

Reflexión final

Internet no es únicamente una herramienta tecnológica.

Es:

- un espacio económico,
- político,

- social,
- cultural,
- jurídico.

Por ello, el marco jurídico de internet busca equilibrar permanentemente:

- libertad y control,
 - innovación y regulación,
 - privacidad y seguridad,
 - soberanía estatal y globalización digital.
-

4. Marco normativo argentino

Ley 27.078 — “Argentina Digital”

Ley 27.078

La Ley 27.078, sancionada en 2014, constituye una de las normas más relevantes del sistema jurídico argentino en materia de telecomunicaciones y tecnologías de la información y las comunicaciones (TIC).

Su finalidad principal es:

garantizar el desarrollo de las telecomunicaciones y asegurar el acceso equitativo a los servicios digitales.

Contexto de aparición

La expansión de internet y de las tecnologías digitales modificó profundamente:

- la comunicación,
- el acceso a la información,
- el comercio,
- la educación,
- los servicios estatales.

Frente a ello, el Estado argentino buscó establecer un marco regulatorio moderno para:

- telecomunicaciones,
 - conectividad,
 - redes digitales,
 - servicios TIC.
-

Objetivos centrales de la ley

La ley procura:

- promover inclusión digital,
 - ampliar acceso a internet,
 - proteger usuarios,
 - garantizar competencia,
 - fortalecer infraestructura tecnológica.
-

Principios fundamentales reconocidos

a) Interés público de las telecomunicaciones

La ley declara de interés público:

- el desarrollo de las TIC,
 - las telecomunicaciones,
 - los recursos asociados.
-

¿Qué implica jurídicamente?

Significa que el Estado:

- puede regular el sector,
 - controlar condiciones de prestación,
 - intervenir para garantizar acceso universal.
-

Fundamento constitucional indirecto

El acceso a internet se vincula actualmente con derechos fundamentales como:

- educación,
 - información,
 - libertad de expresión,
 - participación democrática.
-

Ejemplo práctico

Sin acceso a internet hoy resulta extremadamente difícil:

- estudiar,
- trabajar,
- realizar trámites,

- acceder a servicios públicos,
 - ejercer ciudadanía digital.
-

b) Neutralidad de la red

Uno de los aspectos más importantes de la Ley 27.078 es el reconocimiento de la neutralidad de la red.

Concepto

Los proveedores de internet deben tratar de manera igualitaria:

- contenidos,
 - aplicaciones,
 - servicios,
 - usuarios.
-

Consecuencia práctica

Un proveedor no puede:

- bloquear plataformas,
 - ralentizar servicios,
 - priorizar contenidos pagos,
 - discriminar aplicaciones competidoras.
-

Ejemplo

Un ISP no debería:

- ralentizar Netflix,
 - bloquear YouTube,
 - favorecer una plataforma propia.
-

Importancia jurídica

La neutralidad protege:

- libertad de expresión,
 - competencia digital,
 - innovación tecnológica,
 - igualdad de acceso.
-

c) Acceso equitativo

La ley busca garantizar acceso universal a servicios TIC.

Problema que intenta resolver

La brecha digital.

¿Qué es la brecha digital?

La desigualdad en:

- acceso tecnológico,
 - conectividad,
 - infraestructura,
 - alfabetización digital.
-

Ejemplos

Diferencias entre:

- zonas urbanas y rurales,
 - sectores socioeconómicos,
 - regiones con distinta infraestructura.
-

Importancia social

El acceso desigual a internet genera nuevas formas de exclusión.

Vinculación con derechos humanos

Actualmente numerosos organismos internacionales consideran que el acceso a internet:
es una condición esencial para el ejercicio efectivo de otros derechos fundamentales.

Organismos regulatorios

En Argentina intervienen organismos como:

ENACOM

ENACOM

Regula:

- telecomunicaciones,
 - servicios audiovisuales,
 - conectividad,
 - espectro radioeléctrico.
-

Tensiones contemporáneas

La regulación digital enfrenta conflictos permanentes entre:

Interés	Objetivo
Libertad empresarial	innovación y mercado
Regulación estatal	protección de usuarios
Seguridad	control de contenidos

datos

5. Derecho comparado

El derecho digital presenta enfoques regulatorios diferentes según cada región del mundo.

Los dos modelos más influyentes actualmente son:

- Unión Europea,
 - Estados Unidos.
-

Unión Europea — Digital Services Act (DSA)

Digital Services Act

¿Qué es el DSA?

Es un reglamento europeo destinado a regular plataformas digitales y servicios online.

Entró en vigor para reforzar:

- protección de usuarios,
 - transparencia,
 - responsabilidad de plataformas.
-

Objetivos principales

a) Moderación de contenidos

Las plataformas deben actuar frente a:

- contenidos ilícitos,
 - discursos de odio,
 - desinformación,
 - productos ilegales.
-

b) Transparencia algorítmica

Las grandes plataformas deben informar:

- cómo funcionan sus algoritmos,
 - cómo recomiendan contenidos,
 - cómo priorizan información.
-

Ejemplo

¿Por qué aparece cierto contenido en redes sociales?

El DSA exige mayor transparencia sobre esos mecanismos.

c) Obligaciones reforzadas para grandes plataformas

Las Big Tech poseen obligaciones especiales.

Ejemplos:

- auditorías,
 - gestión de riesgos sistémicos,
 - controles sobre publicidad personalizada.
-

Empresas alcanzadas

Entre otras:

- Google
 - Meta
 - TikTok
 - Amazon
-

Filosofía del modelo europeo

La Unión Europea prioriza:

- protección de derechos fundamentales,
 - privacidad,
 - control regulatorio,
 - responsabilidad empresarial.
-

Estados Unidos — Section 230 CDA

Section 230

Concepto

La Section 230 es una norma fundamental del derecho digital estadounidense.

Establece que las plataformas digitales:

no son, en principio, responsables por contenidos publicados por usuarios.

Finalidad histórica

Promover el crecimiento de internet y proteger innovación tecnológica.

Consecuencia práctica

Las plataformas tienen amplia inmunidad jurídica respecto de publicaciones de terceros.

Ejemplo

Si un usuario publica contenido ofensivo en una red social:

- generalmente la responsabilidad recae sobre el usuario,

- no sobre la plataforma.
-

Impacto global

La Section 230 permitió el enorme crecimiento de:

- redes sociales,
 - plataformas colaborativas,
 - servicios digitales globales.
-

Críticas contemporáneas

Actualmente existen cuestionamientos por:

- fake news,
 - desinformación,
 - discursos extremistas,
 - falta de control de plataformas.
-

Debate jurídico actual

Pregunta central

¿Hasta qué punto las plataformas deben responder por lo que ocurre dentro de ellas?

Comparación de modelos

Modelo europeo	Modelo estadounidense
Mayor regulación	Mayor libertad empresarial
Protección de usuarios	Protección de plataformas
Responsabilidad reforzada	Inmunidad amplia
Control estatal más intenso	Menor intervención estatal
Transparencia algorítmica	Autorregulación empresarial

Diferencia filosófica de fondo

Unión Europea

Parte de la idea de que:

las plataformas deben asumir responsabilidades proporcionales a su poder digital.

Estados Unidos

Prioriza:

libertad de expresión e innovación empresarial con mínima intervención estatal.

Impacto para América Latina

Muchos países latinoamericanos, incluida Argentina, se encuentran en una posición intermedia.

Se observan influencias de ambos modelos:

Influencia europea	Influencia estadounidense
protección de datos	libertad de plataformas
regulación estatal	innovación digital
tutela de usuarios	menor responsabilidad intermediaria

Caso práctico para debate

Supuesto

Una red social recomienda masivamente contenido falso mediante algoritmos.

Preguntas posibles

- ¿Debe responder la plataforma?
 - ¿Existe responsabilidad algorítmica?
 - ¿La moderación afecta libertad de expresión?
 - ¿Debe intervenir el Estado?
-

Reflexión final

El derecho digital contemporáneo enfrenta uno de los mayores desafíos jurídicos de la actualidad:

encontrar equilibrio entre innovación tecnológica, libertad de expresión, protección de usuarios y control del poder de las plataformas digitales.

Internet ya no es solamente un espacio técnico.

Es un espacio:

- económico,
 - político,
 - social,
 - jurídico,
 - geopolítico.
-

Actividad práctica

Caso

“Un gobierno bloquea una plataforma digital durante protestas sociales.”

Preguntas

- ¿Qué derechos podrían afectarse?
 - ¿Existe censura?
 - ¿Qué rol tiene la neutralidad de red?
 - ¿Puede justificarse por seguridad nacional?
-

Gobierno electrónico

1. Concepto

E-Government o Gobierno Electrónico

El gobierno electrónico —también denominado *e-government* o administración digital— consiste en:

la utilización de tecnologías digitales por parte del Estado para gestionar información, prestar servicios públicos, interactuar con ciudadanos y optimizar procedimientos administrativos.

Idea central

El objetivo principal del gobierno electrónico es modernizar el funcionamiento estatal mediante herramientas tecnológicas.

Esto implica transformar:

- trámites,

- comunicaciones,
 - expedientes,
 - sistemas de gestión,
 - acceso a información pública,
 - interacción entre organismos.
-

Evolución histórica

Tradicionalmente, la administración pública funcionaba mediante:

- expedientes en papel,
- trámites presenciales,
- archivos físicos,
- firmas manuscritas,
- procesos burocráticos lentos.

Con la digitalización, los Estados comenzaron a implementar:

- expedientes electrónicos,
 - portales web,
 - firma digital,
 - identidad digital,
 - interoperabilidad entre organismos,
 - automatización administrativa.
-

Definición doctrinaria

Puede definirse al gobierno electrónico como:

“La incorporación estratégica de tecnologías de la información y comunicación en la actividad estatal para mejorar eficiencia, transparencia, acceso y calidad de los servicios públicos.”

Finalidades principales

a) Prestar servicios públicos

El Estado brinda servicios digitales a ciudadanos y empresas.

Ejemplos

- turnos online,
 - pago de impuestos,
 - certificados digitales,
 - licencias electrónicas,
 - consultas previsionales,
 - trámites judiciales electrónicos.
-

Ejemplos argentinos

AFIP

AFIP

Permite:

- facturación electrónica,
 - declaraciones juradas,
 - pagos tributarios,
 - clave fiscal.
-

ANSES

ANSES

Permite:

- consultas previsionales,
 - trámites jubilatorios,
 - asignaciones,
 - historia laboral.
-

Mi Argentina

Mi Argentina

Centraliza:

- documentación digital,
 - credenciales,
 - servicios estatales.
-

b) Gestionar información pública

El Estado administra enormes volúmenes de datos.

Ejemplos

- registros civiles,
 - datos tributarios,
 - información sanitaria,
 - antecedentes judiciales,
 - padrones electorales.
-

Problemas jurídicos asociados

Protección de datos personales

¿Cómo se protege la información estatal?

Seguridad informática

¿Qué ocurre ante un ciberataque?

Confidencialidad

¿Quién puede acceder a la información?

Transparencia

¿Qué datos deben ser públicos?

c) Interactuar con ciudadanos

El gobierno electrónico modifica la relación Estado-ciudadano.

Antes

Relación burocrática:

- presencial,
 - lenta,
 - fragmentada.
-

Ahora

Relación digital:

- inmediata,
 - remota,
 - automatizada,
 - disponible 24/7.
-

Ventajas

- reducción de tiempos,
 - simplificación administrativa,
 - acceso remoto,
 - menor uso de papel,
 - mayor trazabilidad.
-

d) Optimizar procedimientos administrativos

La digitalización busca aumentar eficiencia estatal.

Ejemplos

- expedientes electrónicos,
 - interoperabilidad,
 - automatización,
 - inteligencia de datos,
 - sistemas de gestión digital.
-

Consecuencia jurídica

Los actos administrativos digitales deben mantener:

- legalidad,
- debido proceso,
- autenticidad,

- integridad documental,
 - seguridad jurídica.
-

Características del gobierno electrónico

Característica	Explicación
Digitalización	sustitución de procesos físicos
Interoperabilidad	conexión entre organismos
Automatización	reducción de tareas manuales
Accesibilidad	servicios remotos
Trazabilidad	seguimiento de actuaciones
Transparencia	acceso a información pública

Beneficios del gobierno electrónico

Para el Estado

- mayor eficiencia,
 - reducción de costos,
 - mejor gestión documental,
 - control administrativo.
-

Para ciudadanos

- rapidez,
 - comodidad,
 - acceso remoto,
 - simplificación de trámites.
-

Para empresas

- menor burocracia,
 - digitalización impositiva,
 - agilización comercial.
-

Riesgos y desafíos

Brecha digital

No todas las personas poseen:

- acceso a internet,
 - dispositivos,
 - alfabetización digital.
-

Ciberseguridad

Los sistemas estatales pueden sufrir:

- hackeos,
 - ransomware,
 - filtraciones,
 - robo de datos.
-

Vigilancia estatal

La acumulación masiva de información genera riesgos sobre:

- privacidad,
 - control social,
 - monitoreo excesivo.
-

Dependencia tecnológica

Muchos Estados utilizan infraestructura privada global.

Ejemplo:

- servicios cloud,
 - software extranjero,
 - plataformas privadas.
-

2. Dimensiones del gobierno electrónico

El gobierno electrónico puede analizarse según el tipo de relación digital involucrada.

G2C — Government to Citizen

Gobierno ↔ Ciudadano

Relación digital entre el Estado y las personas.

Objetivo

Facilitar acceso ciudadano a servicios públicos.

Ejemplos

- turnos online,
 - DNI digital,
 - consultas previsionales,
 - licencias electrónicas,
 - portales de salud.
-

Caso argentino

TAD

TAD

Permite realizar trámites administrativos completamente online.

Importancia jurídica

El modelo G2C impacta sobre:

- acceso a derechos,
 - inclusión digital,
 - ciudadanía digital,
 - debido procedimiento administrativo.
-

G2B — Government to Business

Gobierno ↔ Empresas

Relación digital entre Estado y sector privado.

Objetivos

- simplificar actividad económica,
- facilitar cumplimiento normativo,
- mejorar control fiscal.

Ejemplos

- facturación electrónica,
 - licitaciones digitales,
 - registros empresariales,
 - pagos tributarios online.
-

Caso argentino

AFIP digital

AFIP

Permite:

- declaraciones juradas,
 - facturación electrónica,
 - regímenes fiscales digitales.
-

Importancia jurídica

Implica:

- digitalización tributaria,
- trazabilidad financiera,
- automatización de controles.

G2G — Government to Government

Gobierno ↔ Gobierno

Relación digital entre organismos estatales.

Objetivo

Lograr interoperabilidad administrativa.

¿Qué es interoperabilidad?

Capacidad de distintos sistemas estatales para intercambiar información automáticamente.

Ejemplos

- intercambio de bases de datos,
 - validación automática de identidad,
 - conexión entre registros públicos.
-

Ventajas

- reducción de duplicación documental,
 - mayor eficiencia,
 - agilización administrativa.
-

Riesgos jurídicos

Protección de datos

¿Qué organismos pueden compartir información?

Competencia administrativa

¿Quién controla el tratamiento de datos?

Seguridad informática estatal

¿Cómo se protege la información interconectada?

Ejemplo práctico integrador

Caso

Una persona inicia un trámite jubilatorio online.

Intervienen simultáneamente:

Dimensión	Participación
G2C	ciudadano realiza trámite
G2G	organismos cruzan información
G2B	bancos procesan pagos

Reflexión final

El gobierno electrónico no implica solamente “hacer trámites por internet”.

Supone una transformación estructural del funcionamiento estatal.

Esto genera enormes ventajas en:

- eficiencia,
- accesibilidad,
- transparencia,

pero también nuevos desafíos vinculados con:

- privacidad,
- ciberseguridad,
- inclusión digital,
- protección de derechos fundamentales.

Ejemplos

G2C

- ANSES
- Mi Argentina
- turnos digitales

G2B

- AFIP,
- licitaciones electrónicas,
- facturación electrónica.

G2G

- interoperabilidad entre organismos,
 - intercambio de bases estatales.
-

3. Marco normativo argentino del gobierno electrónico

La transformación digital del Estado argentino se desarrolló progresivamente mediante normas orientadas a:

- modernizar la administración pública,
 - digitalizar procedimientos,
 - optimizar servicios,
 - incorporar tecnologías de la información,
 - fortalecer transparencia y acceso ciudadano.
-

Decreto 434/2016

Decreto 434/2016

Objeto del decreto

El Decreto 434/2016 aprobó el:

“Plan de Modernización del Estado”.

Constituye uno de los instrumentos centrales del proceso de digitalización administrativa argentina.

Finalidad principal

Transformar la administración pública mediante:

- incorporación de tecnologías digitales,
- simplificación burocrática,
- digitalización documental,
- interoperabilidad,
- mejora de servicios públicos.

Contexto histórico

La administración tradicional presentaba numerosos problemas:

- excesiva burocracia,
- expedientes en papel,
- lentitud administrativa,
- duplicación documental,
- falta de interoperabilidad,
- costos elevados.

El proceso de modernización buscó reemplazar esos sistemas por herramientas digitales.

Ejes del Plan de Modernización

a) Gestión documental electrónica

Digitalización de:

- expedientes,
 - actuaciones administrativas,
 - archivos públicos,
 - firmas.
-

b) Gobierno abierto

Mayor transparencia estatal mediante:

- acceso a información pública,
 - publicación de datos,
 - participación ciudadana.
-

c) Tramitación digital

Creación de sistemas electrónicos para:

- iniciar trámites,
 - realizar presentaciones,
 - consultar expedientes.
-

d) Interoperabilidad

Conexión entre organismos estatales para compartir información de manera automatizada.

Importancia jurídica

El decreto impulsó la consolidación de:

- expediente electrónico,
 - firma digital,
 - administración sin papel,
 - identidad digital estatal.
-

TAD — Trámites a Distancia

TAD

Concepto

TAD es una plataforma digital que permite realizar trámites administrativos completamente online.

Funciones principales

Iniciar expedientes

Los ciudadanos pueden comenzar actuaciones administrativas electrónicamente.

Presentar documentación

Se pueden adjuntar:

- escritos,
 - formularios,
 - archivos digitales,
 - certificados.
-

Gestionar procedimientos

Permite:

- consultar estados,
 - recibir notificaciones,
 - responder requerimientos,
 - descargar constancias.
-

Impacto jurídico

La plataforma TAD transforma la lógica tradicional del procedimiento administrativo.

Antes

- presencialidad obligatoria,
 - expedientes físicos,
 - tiempos extensos,
 - archivos en papel.
-

Ahora

- gestión remota,
 - expediente digital,
 - trazabilidad electrónica,
 - disponibilidad permanente.
-

Ventajas

Ventaja	Impacto
Agilidad	reducción de tiempos
Accesibilidad	trámites remotos
Trazabilidad	seguimiento digital
Transparencia	control de actuaciones
Menor costo	reducción de papel

Requisitos jurídicos fundamentales

Para que un trámite digital tenga validez jurídica deben garantizarse:

- autenticidad,
 - integridad,
 - confidencialidad,
 - identificación del usuario,
 - seguridad informática.
-

Relación con firma digital

La validez de muchas actuaciones digitales depende de:

Ley 25.506

La firma digital permite:

- acreditar identidad,
 - garantizar autoría,
 - asegurar integridad documental.
-

Datos abiertos

Concepto

La política de datos abiertos implica:

la publicación y disponibilidad de información estatal para acceso, reutilización y análisis por parte de ciudadanos, empresas y organizaciones.

Objetivos

- transparencia,
 - control ciudadano,
 - innovación,
 - participación democrática.
-

¿Qué son datasets?

Conjuntos estructurados de datos digitales.

Ejemplos

- estadísticas públicas,
 - transporte,
 - salud,
 - educación,
 - economía,
 - meteorología,
 - presupuesto estatal.
-

Principios de datos abiertos

Acceso público

La información debe estar disponible para cualquier persona.

Reutilización

Los datos pueden utilizarse para:

- investigación,
 - aplicaciones,
 - análisis,
 - desarrollo tecnológico.
-

Formato interoperable

Los datos deben publicarse en formatos reutilizables.

Beneficios

Transparencia estatal

Permite controlar actividad gubernamental.

Innovación tecnológica

Empresas y desarrolladores pueden crear soluciones basadas en datos públicos.

Participación ciudadana

Facilita análisis social y control democrático.

Problemas jurídicos

Protección de datos personales

No toda información estatal puede publicarse libremente.

Riesgo

La apertura excesiva puede vulnerar:

- privacidad,
 - intimidad,
 - confidencialidad.
-

Ejemplo

Publicar datos médicos identificables sería ilegal.

Relación con la Ley 25.326

Ley 25.326

Limita tratamiento y divulgación de datos personales.

4. Desafíos jurídicos del gobierno electrónico

La digitalización estatal genera importantes beneficios, pero también plantea problemas jurídicos complejos.

Brecha digital

Concepto

La brecha digital consiste en la desigualdad en el acceso y uso de tecnologías digitales.

No todos poseen:

- conectividad,
 - dispositivos,
 - alfabetización digital,
 - infraestructura adecuada.
-

Tipos de brecha digital

Tipo	Ejemplo
Económica	falta de recursos
Geográfica	zonas rurales sin internet
Educativa	dificultad para usar sistemas
Generacional	diferencias etarias

Consecuencia jurídica

El acceso desigual puede afectar:

- igualdad ante la ley,
 - acceso a derechos,
 - debido proceso administrativo.
-

Ejemplo práctico

Si un trámite sólo puede hacerse online:

- personas sin conectividad quedan excluidas.
-

Debate jurídico

Pregunta central

¿Puede el Estado digitalizar completamente servicios sin garantizar acceso universal?

Identidad digital

Concepto

La identidad digital es el conjunto de mecanismos tecnológicos utilizados para identificar personas en entornos electrónicos.

Objetivos

- autenticar usuarios,
 - validar identidad,
 - otorgar seguridad jurídica.
-

Problemas jurídicos

a) Autenticación

¿Cómo se verifica que quien opera es realmente esa persona?

b) Biometría

Uso de:

- huella digital,
 - reconocimiento facial,
 - iris,
 - voz.
-

Riesgos biométricos

Los datos biométricos son extremadamente sensibles.

Si son robados:

- no pueden “cambiarse” como una contraseña.
-

c) Suplantación de identidad

Riesgo de:

- robo de credenciales,
 - phishing,
 - hackeo,
 - falsificación digital.
-

Consecuencias jurídicas

Puede producir:

- fraudes,
 - contratos falsos,
 - acceso ilegítimo,
 - delitos informáticos.
-

Caso contemporáneo

Deepfakes e inteligencia artificial aumentan riesgos de falsificación digital.

Seguridad de la información pública

Concepto

El Estado administra enormes volúmenes de información sensible.

Ejemplos

- datos tributarios,
 - antecedentes,
 - información sanitaria,
 - registros biométricos,
 - expedientes judiciales.
-

Riesgos principales

Filtraciones

Divulgación no autorizada de información.

Ransomware

Secuestro digital de sistemas mediante malware.

Funcionamiento típico

Los atacantes:

- bloquean sistemas,
 - cifran información,
 - exigen pagos para liberarla.
-

Ataques estatales o geopolíticos

Algunos ciberataques poseen:

- motivaciones políticas,
 - espionaje,
 - sabotaje,
 - ciberguerra.
-

Exposición de datos sensibles

La filtración de bases públicas puede afectar:

- privacidad,
 - seguridad,
 - identidad,
 - patrimonio.
-

Importancia jurídica

La seguridad informática estatal ya no es sólo una cuestión técnica.

Es también una obligación jurídica vinculada con:

- protección de derechos fundamentales,
 - responsabilidad estatal,
 - privacidad,
 - deber de custodia de información pública.
-

Principios jurídicos involucrados

Principio	Aplicación
Confidencialidad	acceso restringido
Integridad	datos no alterados
Disponibilidad	sistemas accesibles
Autenticidad	identidad verificada
Trazabilidad	registro de actuaciones

Reflexión final

El gobierno electrónico representa uno de los mayores procesos de transformación del Estado contemporáneo.

Sin embargo, la digitalización no garantiza automáticamente:

- inclusión,
- transparencia,
- seguridad,
- protección de derechos.

Por ello, el desafío jurídico actual consiste en construir un Estado digital que sea simultáneamente:

- eficiente,
 - accesible,
 - seguro,
 - transparente,
 - respetuoso de los derechos fundamentales.
-

5. Ejemplos argentinos

AFIP

AFIP

ANSES

ANSES

Poder Judicial electrónico

Poder Judicial de la Nación

Ejemplos:

- expediente digital,
 - notificaciones electrónicas,
 - firma digital.
-

Cierre

Derecho Informático

- regula relaciones digitales,
 - es transversal y dinámica.
-

Internet

- posee gobernanza compleja,
 - implica tensiones entre libertad y regulación.
-

Gobierno electrónico

- mejora eficiencia estatal,
 - pero genera desafíos de privacidad y seguridad.
-

Adelanto próxima clase

Contratos informáticos y comercio electrónico

Temas:

- clickwrap,
- firma digital,
- contratación online,
- marketplaces,
- responsabilidad de plataformas,
- prueba electrónica.