Clase 1 — Presentación de la materia + Derecho, legislación e informática

- **Eje: para qué necesita Derecho una persona que programa / trabaja en tecnología.**
- **Contenidos: concepto de legislación; concepto de Derecho; relación Derecho–informática; tipos de derecho — público, privado, constitucional, civil, penal, administrativo.**
- **Actividad: mapa de situaciones reales: software, datos, contratos, delitos informáticos, IA, trabajo remoto.**
- **Resultado esperado: que entiendan que la materia no es "memoria legal", sino gestión de riesgos jurídicos en tecnología.**

El *Derecho* puede definirse, en sentido doctrinario, como un *ordenamiento normativo e institucional* que, sustentado en principios y valores, *organiza la convivencia social* mediante la atribución de derechos y la imposición de deberes, y *asegura su vigencia* a través de mecanismos de garantía, sanción y reparación frente al incumplimiento.

Dicho de manera más simple: el Derecho organiza la vida en sociedad.

Nos dice:

- qué podemos hacer;
- qué no podemos hacer;
- qué estamos obligados a hacer;
- qué derechos tenemos;
- qué responsabilidades asumimos;

- qué pasa si incumplimos;
- quién resuelve un conflicto.

Cuando hablamos de Derecho, entonces, no hablamos solamente de leyes. Hablamos de un sistema mucho más amplio.

Ese sistema incluye:

- normas;
- principios;
- instituciones;
- jueces;
- organismos administrativos;
- contratos;
- jurisprudencia;
- doctrina;
- derechos fundamentales;
- mecanismos de responsabilidad.

La doctrina clásica explica esto de distintas maneras. Por ejemplo, *Llambías* entiende el Derecho como un ordenamiento social destinado a regular la conducta humana en sociedad mediante normas obligatorias. *Borda*, por su parte, lo presenta como un sistema necesario para organizar la convivencia y resolver conflictos de intereses.

No necesitamos quedarnos con una definición de memoria. Lo importante es entender la idea: donde hay convivencia, intereses, conflictos, derechos y obligaciones, hay Derecho.

Y en tecnología hay todo eso.

Hay usuarios, empresas, programadores, clientes, datos, dinero, propiedad intelectual, privacidad, seguridad, contratos y responsabilidad.

Por eso la informática no está fuera del Derecho.

Elementos del Derecho

Podemos pensar el Derecho como un sistema formado por cuatro elementos principales.

1. Normas

Las normas son reglas de conducta.

Pueden decir:

- esto está permitido;
- esto está prohibido;
- esto es obligatorio;
- si ocurre esto, corresponde esta consecuencia.

Ejemplo tecnológico: si una persona accede sin autorización a un sistema informático de acceso restringido, esa conducta puede estar sancionada penalmente.

Otro ejemplo: si una empresa trata datos personales, tiene que respetar ciertas reglas de información, consentimiento, finalidad y seguridad.

---

2. Principios

Los principios son criterios generales que orientan la interpretación y aplicación del Derecho.

Algunos principios importantes son:

1. *Buena fe*

Qué es: deber de actuar con lealtad, honestidad y coherencia (sin "jugar sucio" ni sorprender a la otra parte).

Para qué sirve: interpretar contratos, exigir conductas correctas, frenar abusos.

Ejemplo tech: una empresa cambia condiciones de un servicio (precio/alcance) sin avisar o escondido en letra chica. Aunque "esté en los términos", puede discutirse por falta de buena fe.

2. *No dañar a otro*

Qué es: principio básico de responsabilidad: quien causa un daño injustificado debe repararlo.

Para qué sirve: base de daños y perjuicios (civil), incluso sin contrato.

Ejemplo tech: una app filtra datos por mala seguridad y eso genera fraude/hostigamiento a usuarios; hay daño y puede haber responsabilidad.

3. *Razonabilidad*

Qué es: las medidas (del Estado o de privados en ciertos contextos) deben ser lógicas, justificadas y no arbitrarias; proporción entre medio y fin.

Para qué sirve: controlar excesos y decisiones absurdas.

Ejemplo tech: una universidad exige para rendir un examen que el estudiante instale software invasivo que accede a toda la computadora y cámara 24/7, sin necesidad real.

4. *Igualdad*

Qué es: prohibición de discriminación arbitraria; trato igual a quienes están en situación equivalente y trato distinto solo si hay razón objetiva.

Para qué sirve: evaluar sesgos, discriminación, acceso a servicios.

Ejemplo tech: un algoritmo de selección laboral descarta sistemáticamente CVs de determinados barrios/edades; aunque no "quiera" discriminar, el resultado puede violar igualdad.

5. *Privacidad*

Qué es: derecho a la vida privada, a controlar información personal y a no sufrir intromisiones indebidas.

Para qué sirve: limitar recolección/uso de datos, vigilancia y exposición.

Ejemplo tech: una app de linterna pide contactos, micrófono y ubicación; no hay necesidad funcional → problema de privacidad.

6. *Proporcionalidad*

Qué es: test más "técnico" que la razonabilidad: la medida debe ser (i) idónea, (ii) necesaria (no hay alternativa menos lesiva), y (iii) equilibrada (beneficio > costo sobre derechos).

Para qué sirve: evaluar vigilancia, sanciones, recolección de datos, restricciones.

Ejemplo tech: para evitar fraude, una plataforma pide foto de DNI + biometría + acceso a galería completa. Puede ser desproporcionado si se podía validar identidad con métodos menos invasivos.

7. *Seguridad jurídica*

Qué es: previsibilidad y estabilidad: que las reglas sean claras, accesibles y relativamente constantes; que la gente pueda planificar su conducta.

Para qué sirve: evitar "cambios sorpresa", ambigüedad normativa y decisiones contradictorias.

Ejemplo tech: una plataforma cambia políticas de moderación sin criterios claros y sanciona cuentas sin explicar por qué; afecta previsibilidad y confianza.

8. *Protección del consumidor*

Qué es: principio que protege a la parte más débil en relaciones de consumo (usuarios/clientes), imponiendo deberes reforzados a proveedores: información clara, trato digno, garantías, seguridad, no cláusulas abusivas.

Para qué sirve: controlar publicidad engañosa, suscripciones trampa, términos abusivos, fallas de producto/servicio.

Ejemplo tech: "free trial" que en realidad cobra automáticamente sin aviso claro y con cancelación escondida → típico tema de consumo.

9. *Tutela judicial efectiva*

Qué es: derecho real (no solo teórico) a acceder a un juez, ser oído, tener un proceso útil y una decisión en tiempo razonable, con posibilidad de ejecución.

Para qué sirve: frenar obstáculos para reclamar derechos.

Ejemplo tech: una plataforma bloquea una cuenta y el único "reclamo" es un formulario automático sin revisión humana ni respuesta; si impacta derechos/medios de vida, puede discutirse si hay vías efectivas de reclamo.

En tecnología, los principios son fundamentales porque muchas veces la realidad avanza más rápido que las leyes.

Por ejemplo: quizás no haya una norma específica para cada caso de inteligencia artificial, pero sí existen principios aplicables: no discriminación, privacidad, transparencia, responsabilidad, buena fe, deber de información.

---

3. Instituciones

El Derecho también necesita instituciones que lo apliquen.

Por ejemplo:

1. *Poder Judicial*

Ejemplo: una persona demanda a una empresa porque se filtraron sus datos (acción de daños + medida cautelar para que bajen/publiciten el incidente). El juez ordena preservar logs, bloquear accesos y eventualmente indemnizar.

Otro: amparo/hábeas data para que una plataforma rectifique o elimine datos incorrectos.

2. *Congreso*

Ejemplo: sanciona una ley que crea obligaciones para plataformas (p. ej., reglas de ciberseguridad para "infraestructura crítica", o actualización del régimen de datos personales).

Impacto práctico: cambia qué debe tener tu sistema (consentimiento, seguridad, plazos de conservación, auditorías, etc.).

3. *Organismos administrativos* (Ministerios, Secretarías, entes reguladores, etc.)

Ejemplo: una empresa recibe una inspección y un sumario administrativo por incumplir normativa de seguridad en un servicio digital.

Otro: un organismo dicta una disposición/reglamentación técnica (p. ej., requisitos para trámites digitales, firma electrónica, resguardo documental).

4. *Autoridad de protección de datos* (en Argentina, la AAIP)

Ejemplo: un usuario denuncia a una app por recolectar datos excesivos o por no permitir ejercer derechos de acceso/supresión. La autoridad investiga, intima a adecuar políticas, puede sancionar y ordenar medidas correctivas.

Otro: ante una brecha, puede exigir plan de remediación (seguridad, minimización, transparencia).

5. *Defensorías del consumidor* (y oficinas/autoridades de defensa del consumidor)

Ejemplo: reclamo por suscripción "trampa" en una plataforma (free trial que cobra sin aviso claro) o por falta de botón de baja. Se cita a audiencia, se ordena reintegro, se aplican sanciones.

Otro: un marketplace no responde por una estafa y el usuario reclama por trato indigno / información insuficiente.

6. *Fiscalías*

Ejemplo: denuncia penal por phishing/ransomware: la fiscalía investiga, pide informes a proveedores, ordena medidas urgentes para preservar evidencia digital.

Otro: acceso ilegítimo a una cuenta o sistema (investigación por delito informático).

7. *Organismos de control* (según sector: BCRA, CNV, ENACOM, superintendencias, etc.)

Ejemplo fintech: el regulador exige estándares de seguridad, continuidad operativa y gestión de incidentes; ante fallas, abre sumario y sanciona.

Ejemplo telecom: control de obligaciones del proveedor de internet/servicios de comunicaciones.

8. *Registros públicos*

Ejemplo: Registro Nacional de Bases de Datos (si corresponde), o registros societarios (IGJ/Registros Provinciales) para constituir una empresa de software.

Ejemplo probatorio: registro/marca del nombre de una app o inscripción de contratos/actos que luego sirven para acreditar derechos (según el caso).

Si me decís *para cuál clase* lo querés (Clase 1 o Clase 2) y *qué formato* (2 líneas por ítem vs. mini-casos de 5–6 líneas), te lo dejo listo para pegar en el apunte.

En tecnología, esto aparece cuando, por ejemplo, hay una denuncia por filtración de datos, una investigación por fraude informático, una demanda por incumplimiento contractual o una sanción administrativa por tratamiento indebido de información.

---

4. Consecuencias jurídicas

El incumplimiento de una norma puede generar consecuencias.

Por ejemplo:

- obligación de reparar daños;

- multas;
- sanciones administrativas;
- responsabilidad penal;
- nulidad de un contrato;
- obligación de cesar una conducta;
- indemnización;
- pérdida de confianza o daño reputacional.

En informática, muchas veces se piensa solo en el riesgo técnico. Pero un incidente también puede tener consecuencias jurídicas.

Una filtración de datos no es solo "un problema de seguridad". Puede ser:

- un incumplimiento contractual;
- una violación de la Ley de Protección de Datos Personales;
- una fuente de responsabilidad civil;
- un daño reputacional;
- eventualmente, un hecho investigable penalmente si hubo acceso ilegítimo.

---

3. Artículos constitucionales importantes para tecnología

Ahora vamos a ver algunos artículos de la Constitución Nacional que nos sirven como base.

No vamos a estudiar Derecho Constitucional en profundidad, pero sí necesitamos entender que muchos problemas tecnológicos afectan derechos constitucionales.

Artículo 19 de la Constitución Nacional

El artículo 19 dice:

> "Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están solo reservadas a Dios, y exentas de la autoridad de los magistrados."

Este artículo es central para pensar privacidad, autonomía personal y límites a la intervención del Estado o de terceros.

Llevado a tecnología, nos permite preguntar:

- ¿hasta dónde puede una empresa recolectar información sobre una persona?
- ¿hasta dónde puede una app rastrear ubicación?
- ¿hasta dónde puede una plataforma monitorear actividad?
- ¿hasta dónde puede el Estado usar sistemas de vigilancia?
- ¿qué parte de nuestra vida digital pertenece al ámbito privado?

Ejemplo: una app de linterna que pide acceso a ubicación, contactos, micrófono y cámara. Técnicamente puede pedirlo. Pero jurídicamente tenemos que preguntarnos: ¿es necesario? ¿es proporcional? ¿el usuario lo sabe? ¿presta consentimiento real? ¿para qué se usan esos datos?

Artículo 18 de la Constitución Nacional

El artículo 18 protege, entre otras cosas, la defensa en juicio, el debido proceso y la inviolabilidad del domicilio, correspondencia y papeles privados.

Cuando la Constitución habla de correspondencia y papeles privados, tenemos que leer esa protección también en clave actual.

Hoy nuestra vida privada no está solamente en cartas o papeles. Está en:

- correos electrónicos;
- chats;
- archivos en la nube;
- celulares;
- computadoras;
- bases de datos;
- cuentas;
- mensajes;
- historiales;
- credenciales;
- documentación digital.

Entonces, si alguien accede sin autorización a una cuenta, extrae información, revisa mensajes o copia archivos privados, puede haber una afectación de derechos constitucionales y también consecuencias civiles o penales.

Artículo 43 de la Constitución Nacional — Habeas data

El artículo 43 incorpora la acción de habeas data.

Esta acción permite que una persona pueda tomar conocimiento de los datos que sobre ella existan en registros o bancos de datos públicos o privados

destinados a proveer informes, y en caso de falsedad o discriminación exigir supresión, rectificación, confidencialidad o actualización.

Este artículo es muy importante para la informática.

Porque vivimos en una sociedad de bases de datos.

Tenemos datos en:

- bancos;
- plataformas;
- redes sociales;
- organismos públicos;
- sistemas de salud;
- universidades;
- empresas;
- empleadores;
- sistemas de scoring;
- billeteras virtuales;
- comercios electrónicos.

El habeas data permite preguntar:

- ¿qué datos tienen sobre mí?
- ¿para qué los usan?
- ¿son correctos?
- ¿están actualizados?
- ¿pueden compartirse?
- ¿puedo pedir que se rectifiquen?
- ¿puedo pedir que se supriman?

Ejemplo informático: una persona aparece en una base de datos como deudora, pero la deuda está cancelada. Ese dato incorrecto le impide acceder a un crédito. Ahí puede aparecer un reclamo de habeas data.

Otro ejemplo: una plataforma conserva datos personales mucho tiempo después de que el usuario dejó de usar el servicio. Hay que analizar si corresponde conservarlos, por cuánto tiempo y con qué finalidad.

---

4. Jurisprudencia inicial: tecnología y derechos

Vamos a mencionar algunos casos jurisprudenciales importantes. No para estudiarlos en detalle todavía, sino para entender que estos temas ya llegaron a los tribunales.

Caso "Halabi" — CSJN, 2009

En el caso *Halabi, Ernesto c/ Poder Ejecutivo Nacional*, la Corte Suprema analizó una cuestión vinculada con intervención de comunicaciones y protección de la privacidad.

¿Por qué nos importa?

Porque muestra que una medida tecnológica puede afectar derechos de muchas personas al mismo tiempo.

La Corte reconoció allí la dimensión colectiva de ciertos derechos vinculados a la privacidad y a las comunicaciones.

Para nuestra materia, la idea clave es esta:

> La tecnología puede afectar derechos de manera masiva. No siempre el daño tecnológico es individual. A veces un sistema, una base de datos o una política de vigilancia impacta sobre miles o millones de personas.

Caso “Rodríguez, María Belén c/ Google” — CSJN, 2014

Este caso trató la responsabilidad de buscadores de internet frente a contenidos que afectaban derechos personalísimos, como imagen, honor e intimidad.

La Corte discutió el rol de los intermediarios tecnológicos.

Nos sirve para pensar:

- buscadores;
- plataformas;
- intermediarios;
- contenidos de terceros;
- libertad de expresión;
- derecho al honor;
- derecho a la imagen;
- responsabilidad.

La idea pedagógica para hoy es:

> No toda plataforma responde automáticamente por todo contenido de terceros, pero puede haber responsabilidad si toma conocimiento efectivo de una afectación concreta y no actúa según corresponde.

Caso “Denegri c/ Google” — CSJN, 2022

En este caso se discutió el llamado “derecho al olvido” frente a resultados de búsqueda vinculados a hechos antiguos.

La Corte rechazó una aplicación amplia del derecho al olvido en ese caso, poniendo énfasis en la libertad de expresión y en el interés público de la información.

Este caso nos sirve para pensar:

- memoria digital;
- reputación online;
- buscadores;
- privacidad;
- interés público;
- tensión entre derechos.

En tecnología, muchas veces no hay un solo derecho involucrado. Hay tensiones.

Por ejemplo:

- privacidad vs. libertad de expresión;
- seguridad vs. intimidad;
- innovación vs. protección de datos;
- automatización vs. no discriminación;
- eficiencia empresarial vs. derechos laborales.

El Derecho ayuda a ordenar esas tensiones.

5. ¿Qué es la legislación?

Ahora pasamos al segundo concepto central.

Legislación — definición

La *legislación* es el conjunto de leyes dictadas por los órganos competentes del Estado.

Es decir, cuando hablamos de legislación, hablamos de normas escritas, formalmente sancionadas.

Pero atención: legislación y Derecho no son exactamente lo mismo.

La legislación es una parte del Derecho, pero el Derecho es más amplio.

Diferencia entre Derecho y legislación

Podemos verlo así:

El Derecho incluye:

- leyes;
- Constitución;
- tratados;
- principios;
- jurisprudencia;
- contratos;

- doctrina;
- instituciones.

La legislación, en cambio, se refiere principalmente a las leyes y normas dictadas por órganos competentes.

Entonces, si una persona pregunta: "¿qué ley regula esto?", esa pregunta puede ser útil, pero a veces es insuficiente.

En tecnología pasa mucho.

Por ejemplo, frente a un problema de inteligencia artificial, quizás no exista una ley argentina completa y específica para ese caso concreto. Pero eso no significa que no haya Derecho aplicable.

Puede haber:

- Constitución Nacional;
- Ley de Protección de Datos Personales;
- Código Civil y Comercial;
- Ley de Defensa del Consumidor;
- Código Penal;
- normas laborales;
- contratos;
- principios de responsabilidad;
- jurisprudencia;
- estándares técnicos;
- doctrina especializada.

Código Civil y Comercial — Artículos 1 y 2

El Código Civil y Comercial nos da una pauta muy importante.

Artículo 1

Establece que los casos deben resolverse según las leyes aplicables, conforme con la Constitución Nacional y los tratados de derechos humanos.

Esto significa que ninguna ley se interpreta aislada. Siempre se interpreta dentro de un sistema.

Artículo 2

Indica que la ley debe interpretarse teniendo en cuenta sus palabras, sus finalidades, las leyes análogas, los tratados de derechos humanos, los principios y los valores jurídicos.

¿Por qué esto importa en informática?

Porque la tecnología cambia más rápido que las leyes.

Entonces, ante casos nuevos, muchas veces hay que razonar jurídicamente usando:

- normas generales;
- principios;
- analogías;
- finalidad de la norma;
- derechos constitucionales;
- criterios jurisprudenciales.

Ejemplo: deepfakes.

Quizás no encontremos una única ley que diga “deepfake” en todos los supuestos posibles. Pero sí podemos analizar:

- derecho a la imagen;
- derecho al honor;
- protección de datos;
- violencia digital;
- responsabilidad civil;
- delito, si hay extorsión, amenazas, fraude o suplantación;
- propiedad intelectual;
- daño moral.

Doctrina: el Derecho frente al cambio tecnológico

Autores contemporáneos como *Ricardo Lorenzetti* han trabajado la idea de que el Derecho debe responder a sociedades cada vez más complejas, atravesadas por tecnología, consumo, redes, información y nuevos riesgos.

Esto nos sirve para entender una idea central:

> La tecnología no elimina al Derecho. Lo obliga a adaptarse.

Pero también obliga a quienes trabajan en tecnología a comprender mejor el impacto de sus decisiones.

Un programador no necesita saber todo el Derecho. Pero sí necesita detectar alertas.

Por ejemplo:

- “Estoy pidiendo datos que quizás no necesito.”

- “Estoy usando una librería sin revisar licencia.”
- “Estoy guardando contraseñas de forma insegura.”
- “Estoy automatizando una decisión que puede afectar derechos.”
- “Estoy desarrollando sin contrato.”
- “Estoy trabajando con datos de salud.”
- “Estoy implementando IA sin explicar sus límites.”
- “Estoy procesando datos de menores.”

Esa alerta profesional es uno de los objetivos de la materia.

---

6. Relación Derecho–informática

Ahora vamos a ordenar la relación entre Derecho e informática.

Podemos verla desde tres perspectivas.

---

1. La informática como objeto regulado

La informática es objeto del Derecho cuando la ley regula actividades tecnológicas.

Ejemplos:

- protección de datos personales;
- delitos informáticos;
- firma digital;
- comercio electrónico;
- propiedad intelectual del software;

- contratos informáticos;
- ciberseguridad;
- plataformas digitales;
- inteligencia artificial.

Ley 25.326 — Protección de Datos Personales

Esta ley es fundamental para cualquier persona que trabaje con sistemas.

Artículo 1

La ley tiene por objeto proteger integralmente los datos personales asentados en archivos, registros, bancos de datos u otros medios técnicos de tratamiento de datos, sean públicos o privados destinados a dar informes.

Esto significa que si desarrollamos un sistema que almacena datos personales, no estamos simplemente guardando información. Estamos tratando datos protegidos jurídicamente.

Artículo 2 — Datos personales y datos sensibles

La ley define dato personal como información de cualquier tipo referida a personas determinadas o determinables.

Ejemplos:

- nombre;
- DNI;

- correo;
- teléfono;
- domicilio;
- IP, según contexto;
- usuario;
- foto;
- ubicación;
- historial de compras;
- datos laborales;
- datos académicos.

También define datos sensibles: aquellos que revelan origen racial o étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical, información referente a salud o vida sexual.

Ejemplo: una app médica maneja datos sensibles. No es lo mismo que una app que guarda una lista de tareas.

Por eso, desde el diseño del sistema, hay que pensar:

- qué datos pido;
- por qué los pido;
- dónde los guardo;
- quién accede;
- por cuánto tiempo;
- cómo los protejo;
- qué informo al usuario.

Artículo 5 — Consentimiento

La ley exige consentimiento para el tratamiento de datos personales, salvo excepciones.

Esto no significa poner cualquier cartel y listo.

El consentimiento debe estar vinculado a información clara sobre:

- qué datos se recolectan;
- para qué se usan;
- quién los trata;
- si se comparten;
- cómo ejercer derechos;
- qué consecuencias tiene no brindarlos.

Ejemplo: si una app dice “acepto términos y condiciones” pero nunca explica que va a compartir datos con terceros para publicidad, puede haber un problema.

Artículo 9 — Seguridad

El artículo 9 exige adoptar medidas técnicas y organizativas necesarias para garantizar seguridad y confidencialidad.

Esto es importantísimo para estudiantes de programación.

Porque seguridad no es solo una recomendación técnica. También puede ser una obligación jurídica.

Medidas concretas:

- control de accesos;
- roles y permisos;

- cifrado;
- contraseñas adecuadamente protegidas;
- hash y salt;
- backups;
- logs;
- monitoreo;
- actualización de dependencias;
- prevención de inyecciones SQL;
- protección de APIs;
- mínima recolección de datos;
- mínima exposición de privilegios;
- plan de respuesta a incidentes.

Cuando un sistema está mal diseñado y expone datos, no es solo "un bug". Puede ser una infracción legal.

---

2. La informática como herramienta del Derecho

La informática también transformó el trabajo jurídico.

Hoy tenemos:

- expedientes digitales;
- firma digital;
- notificaciones electrónicas;
- audiencias remotas;
- bases de jurisprudencia;
- sistemas de gestión;
- automatización documental;
- inteligencia artificial aplicada a búsqueda y análisis;

- plataformas de trámites;
- gobierno digital.

Un ejemplo es la firma digital.

Ley 25.506 — Firma Digital

Esta ley regula la firma digital y su eficacia jurídica.

La idea central es que una firma digital permite verificar:

- identidad del firmante;
- integridad del documento;
- autenticidad;
- no alteración posterior.

Esto es una intersección clara entre técnica y Derecho.

La criptografía permite una función jurídica: dar validez, confianza e integridad a documentos digitales.

---

3. La informática como fuente de riesgos jurídicos

La tercera forma de relación es la más práctica para ustedes.

La informática genera riesgos jurídicos.

Ejemplos:

Riesgos sobre datos

- filtración;
- tratamiento sin consentimiento;
- venta indebida;
- perfilamiento;
- uso para fines no informados;
- datos sensibles mal protegidos.

Riesgos contractuales

- falta de contrato;
- alcance ambiguo;
- entregas no definidas;
- soporte no pactado;
- falta de pago;
- propiedad del código;
- confidencialidad.

Riesgos penales

- acceso ilegítimo;
- fraude informático;
- phishing;
- daño informático;
- ransomware;
- suplantación de identidad.

Riesgos de inteligencia artificial

- respuestas falsas;
- sesgos;

- decisiones opacas;
- discriminación;
- uso indebido de datos;
- falta de supervisión humana;
- daños por automatización.

Riesgos laborales

- monitoreo excesivo;
- control remoto;
- geolocalización;
- capturas de pantalla;
- productividad algorítmica;
- trabajo para clientes del exterior;
- propiedad intelectual del código producido.

---

7. Tipos de Derecho aplicados a tecnología

Ahora vamos a ver ramas básicas del Derecho, siempre con ejemplos informáticos.

Derecho público

El *Derecho público* regula relaciones donde interviene el Estado en ejercicio de poder público o donde está comprometido un interés general.

Ejemplos:

- regulación estatal de datos personales;
- delitos informáticos;
- contratación pública de software;
- sistemas de vigilancia;
- trámites digitales;
- sanciones administrativas;
- ciberseguridad estatal;
- acceso a información pública.

Ejemplo: un municipio contrata un sistema de cámaras con reconocimiento facial.

Ahí hay Derecho público porque interviene el Estado y se afectan intereses generales: seguridad, privacidad, datos biométricos, control ciudadano, transparencia y posibles abusos.

Preguntas jurídicas:

- ¿cuál es la finalidad?
- ¿qué datos se recolectan?
- ¿cuánto tiempo se guardan?
- ¿quién accede?
- ¿hay control?
- ¿qué pasa con falsos positivos?
- ¿existe discriminación algorítmica?
- ¿la medida es proporcional?

Derecho privado

El *Derecho privado* regula relaciones entre particulares.

Ejemplos:

- contrato entre programador y cliente;
- contrato de software;
- licencia SaaS;
- términos y condiciones;
- propiedad intelectual;
- responsabilidad por fallas;
- confidencialidad;
- relación entre plataforma y usuario.

Código Civil y Comercial — Art. 958

Este artículo reconoce la libertad contractual: las partes son libres para celebrar contratos y determinar su contenido dentro de los límites de la ley, el orden público, la moral y las buenas costumbres.

Aplicado a tecnología:

Si desarrollo software para un cliente, puedo pactar:

- precio;
- alcance;
- plazos;
- entregables;
- soporte;
- mantenimiento;
- propiedad del código;
- uso de librerías;
- confidencialidad;
- garantías;
- responsabilidad;

- forma de pago.

Pero si no lo pacto, después aparece el conflicto.

Ejemplo: el cliente dice “yo pagué, el código es mío”. La persona programadora dice “no, yo te di una licencia de uso, pero el código fuente sigue siendo mío”. Si no hay contrato, el problema queda abierto.

Derecho constitucional

El *Derecho constitucional* reconoce derechos fundamentales y organiza el poder del Estado.

En tecnología aparece todo el tiempo:

- privacidad;
- igualdad;
- libertad de expresión;
- propiedad;
- defensa;
- debido proceso;
- habeas data;
- no discriminación;
- acceso a información.

Ejemplo: un algoritmo de selección laboral descarta automáticamente candidatos de determinada edad, barrio o género.

Puede haber un problema de igualdad y discriminación.

Aunque nadie haya programado “discriminar”, el sistema puede producir un resultado discriminatorio por los datos usados o por el entrenamiento del modelo.

Pregunta clave:

> ¿La decisión técnica produce un impacto injusto sobre derechos?

Derecho civil

El *Derecho civil* regula contratos, obligaciones, daños, responsabilidad y derechos personalísimos.

Código Civil y Comercial — Art. 1716

Este artículo establece que la violación del deber de no dañar a otro o el incumplimiento de una obligación da lugar a la reparación del daño causado.

Aplicado a informática:

Si una empresa desarrolla un sistema inseguro y por esa falla se pierden datos o se causa un perjuicio económico, puede haber responsabilidad civil.

Ejemplos:

- pérdida de información de clientes;
- caída de sistema crítico;
- exposición de datos personales;
- incumplimiento de entrega;
- software defectuoso;
- uso no autorizado de imagen;

- falla en sistema de pagos.

Código Civil y Comercial — Art. 53

Protege derechos personalísimos como imagen, voz, intimidad, honor e identidad.

Aplicado a tecnología:

- deepfakes;
- uso de fotos sin permiso;
- perfiles falsos;
- exposición de intimidad;
- publicaciones virales;
- manipulación de imagen;
- daño reputacional.

Derecho penal

El *Derecho penal* define delitos y penas.

No todo problema informático es delito. Esto es muy importante.

Si entrego tarde un software, probablemente sea un problema contractual.

Si entro sin permiso a una base de datos, puede ser un delito.

La Ley 26.388 incorporó y modificó figuras vinculadas a delitos informáticos en el Código Penal.

Código Penal — Art. 153 bis

Sanciona el acceso ilegítimo a un sistema o dato informático de acceso restringido.

Ejemplo:

- entrar a una cuenta ajena;
- acceder a un panel administrativo sin autorización;
- usar credenciales de otra persona;
- exceder permisos otorgados;
- ingresar a una base de datos restringida.

Aunque la persona no robe información, el acceso no autorizado ya puede ser jurídicamente relevante.

Código Penal — Art. 173 inc. 16

Regula supuestos de defraudación mediante manipulación informática o técnica semejante.

Ejemplos:

- phishing;
- manipulación de sistemas de pago;
- engaños digitales;
- uso fraudulento de credenciales;
- alteración de operaciones para obtener beneficio económico.

Daño informático

El Código Penal también contempla daños sobre datos, documentos, programas o sistemas.

Ejemplos:

- borrar información;
- introducir malware;
- alterar archivos;
- destruir bases de datos;
- inutilizar sistemas.

La idea central para ustedes:

> La seguridad informática no es solo una buena práctica técnica. También tiene relevancia penal, civil, contractual y reputacional.

Derecho administrativo

El *Derecho administrativo* regula la actividad del Estado y su relación con particulares.

Ejemplos tecnológicos:

- licitaciones de software;
- contratación estatal;
- expediente electrónico;
- firma digital en trámites;
- sanciones administrativas;
- sistemas públicos;
- acceso a información pública;
- protección de datos en organismos estatales.

Ley 19.549 — Procedimiento Administrativo Nacional

Regula procedimientos ante la Administración Pública Nacional.

Aplicado a tecnología:

Cuando hacemos trámites digitales, notificaciones electrónicas o presentaciones por plataformas estatales, hay reglas jurídicas sobre:

- validez;
- plazos;
- notificaciones;
- recursos;
- actos administrativos;
- expediente;
- prueba digital.

Ley 27.275 — Acceso a la Información Pública

Reconoce el derecho de acceso a información pública.

Aplicado a informática:

Los sistemas del Estado deberían permitir trazabilidad, transparencia y acceso a información pública, con límites razonables por privacidad, datos sensibles o seguridad.

---

8. Actividad práctica

Como la clase es de 120 minutos, esta actividad puede hacerse en 15 minutos si venís bien de tiempo, o dejarla iniciada y completar la puesta en común al inicio de la clase siguiente.

Consigna

Vamos a aplicar lo visto.

Cada grupo elige una situación tecnológica y completa este mapa:

Mapa de situación jurídico-tecnológica

1. ¿Cuál es la situación tecnológica?
2. ¿Quiénes intervienen?
3. ¿Qué datos aparecen?
4. ¿Hay contrato o relación jurídica?
5. ¿Qué puede salir mal?
6. ¿Qué rama del Derecho aparece?
7. ¿Qué norma, principio o derecho puede estar involucrado?
8. ¿Qué medida preventiva tomarían?

Caso A — App de turnos médicos

Una clínica encarga una app para turnos, estudios y recordatorios.

Análisis esperado:

- Hay datos personales.
- Hay datos sensibles de salud.
- Aplica Ley 25.326.
- Importan consentimiento, finalidad y seguridad.
- Puede haber responsabilidad civil si se filtra información.
- Deben existir accesos restringidos, confidencialidad y medidas técnicas.

Normas:

- Ley 25.326, arts. 2, 5 y 9.
- Art. 19 CN.
- Art. 43 CN.
- CCCN art. 1716.

Caso B — Marketplace de productos usados

Una plataforma permite comprar y vender productos.

Análisis esperado:

- Hay usuarios, pagos, publicaciones, reputación.
- Puede haber estafas.
- Puede haber responsabilidad de plataforma.
- Aparecen consumidores, contratos y eventualmente delitos.

Ramas:

- civil;
- comercial;
- consumidor;
- penal.

Medidas preventivas:

- términos y condiciones claros;
- verificación de identidad;
- sistema de reclamos;
- trazabilidad;

- prevención de fraude.

Caso C — Sistema de control horario remoto

Una empresa instala software que toma capturas de pantalla y mide actividad.

Análisis esperado:

- Hay privacidad laboral.
- Puede haber vigilancia excesiva.
- Hay tratamiento de datos personales.
- Debe haber proporcionalidad.
- Debe informarse al trabajador.

Normas/principios:

- Art. 19 CN.
- Ley 25.326.
- Derecho laboral.
- Proporcionalidad y razonabilidad.

Caso D — Chatbot de IA

Una empresa usa un chatbot para responder consultas de clientes.

Análisis esperado:

- Puede dar respuestas erróneas.
- Puede recolectar datos personales.

- Puede generar responsabilidad.
- Debe informar límites.
- Debe haber supervisión humana en temas sensibles.

Ramas:

- civil;
- consumidor;
- datos personales;
- constitucional.

Medidas:

- disclaimers claros;
- no pedir datos sensibles innecesarios;
- revisión humana;
- registro de errores;
- política de privacidad.

Caso E — Software freelance sin contrato

Una persona desarrolla un sistema para un cliente sin contrato escrito.

Análisis esperado:

- No está claro el alcance.
- No está claro el precio.
- No está claro quién es dueño del código.
- No está claro el mantenimiento.
- Puede haber conflicto.

Normas:

- CCCN art. 958.
- Responsabilidad contractual.
- Propiedad intelectual.

Medidas:

- contrato;
- alcance funcional;
- entregables;
- fechas;
- propiedad del código;
- confidencialidad;
- soporte.

---

9. Cierre de la clase

Para cerrar, quiero que se lleven una idea simple.

La materia no consiste en memorizar leyes. Si se quedan solamente con artículos de memoria, la materia no sirve.

La materia sirve si ustedes aprenden a detectar riesgos.

Cuando estén frente a un sistema, una app, una base de datos, un contrato, una plataforma o una herramienta de inteligencia artificial, quiero que puedan preguntarse:

- ¿qué datos se tratan?
- ¿quiénes son los usuarios?

- ¿qué derechos pueden verse afectados?
- ¿qué obligaciones existen?
- ¿qué puede salir mal?
- ¿quién responde?
- ¿hay contrato?
- ¿hay consentimiento?
- ¿hay seguridad suficiente?
- ¿hay posibilidad de daño?
- ¿hay riesgo penal?
- ¿hay riesgo de discriminación?
- ¿qué medida preventiva puedo tomar?

Esa mirada es profesional.

Una persona que trabaja en tecnología no necesita saber todo el Derecho. Pero sí necesita saber cuándo una decisión técnica puede generar un problema jurídico.

Ese va a ser el enfoque de la materia: *gestión de riesgos jurídicos en tecnología*.

---

10. Tarea para la próxima clase

Para la próxima clase, elegir una aplicación, plataforma o sistema digital que usen habitualmente y responder en media carilla o en bullets:

1. ¿Qué datos recolecta?
2. ¿Hay datos personales o sensibles?
3. ¿Qué contrato, términos o condiciones aceptan al usarla?
4. ¿Qué problema jurídico podría aparecer?
5. ¿Qué rama del Derecho estaría involucrada?

6. ¿Qué medida preventiva debería existir?

La idea no es que hagan un trabajo jurídico perfecto. La idea es que empiecen a mirar tecnología con una mirada distinta: técnica, pero también jurídica y preventiva.

---

11. Versión ultra breve para cerrar oralmente

> "Cada línea de código puede tener consecuencias fuera del código. Puede afectar datos, derechos, contratos, dinero, privacidad, seguridad o responsabilidad. Esta materia existe para que aprendan a ver eso antes de que el problema explote."

---

12. Apunte final

Clase 1 — Ideas principales

1. El Derecho regula la convivencia social mediante normas, principios e instituciones.
2. La legislación es el conjunto de leyes dictadas por órganos competentes, pero no agota el Derecho.
3. La informática se relaciona con el Derecho porque:
    - es objeto de regulación;
    - es herramienta del Derecho;
    - genera riesgos jurídicos.
4. Las principales áreas jurídicas vinculadas a tecnología son:

- protección de datos;
- contratos;
- responsabilidad civil;
- delitos informáticos;
- propiedad intelectual;
- derecho del consumidor;
- derecho laboral;
- derecho administrativo;
- derechos constitucionales.

5. La materia no busca memoria legal, sino criterio profesional para gestionar riesgos.

Normas vistas

- Constitución Nacional: arts. 18, 19 y 43.
- Código Civil y Comercial: arts. 1, 2, 53, 958 y 1716.
- Ley 25.326: arts. 1, 2, 5 y 9.
- Ley 25.506: firma digital.
- Ley 26.388: delitos informáticos.
- Código Penal: art. 153 bis y art. 173 inc. 16.
- Ley 19.549: procedimiento administrativo.
- Ley 27.275: acceso a la información pública.

Jurisprudencia mencionada

- CSJN, *Halabi, Ernesto c/ PEN*, 2009.
- CSJN, *Rodríguez, María Belén c/ Google Inc.*, 2014.
- CSJN, *Denegri, Natalia Ruth c/ Google Inc.*, 2022.

Doctrina mencionada

- Llambías: Derecho como ordenamiento social regulador de la conducta humana.
- Borda: Derecho como sistema de organización de convivencia y resolución de conflictos.
- Lorenzetti: necesidad de interpretar el Derecho frente a nuevas realidades sociales, tecnológicas y de consumo.