CLASE 14: DELITOS INFORMÁTICOS, EVIDENCIA DIGITAL Y RESPONSABILIDAD DE LOS INTERMEDIARIOS DE INTERNET

Carrera: Tecnicatura Universitaria en Programación – UTN

Duración: 120 minutos

Unidad temática: Derecho Informático

OBJETIVOS DE LA CLASE

Al finalizar la clase, el estudiante será capaz de:

- Comprender qué es un delito informático y cuáles son sus características.
- Identificar los principales delitos incorporados por la Ley 26.388.
- Diferenciar autenticación de autorización desde una perspectiva jurídica y técnica.
- Reconocer la importancia de la evidencia digital y de la cadena de custodia.
- Comprender la responsabilidad de buscadores, proveedores de hosting, ISPs y plataformas digitales.
- Analizar casos reales aplicando normas jurídicas y criterios técnicos.
- Comprender la importancia del Convenio de Budapest para la persecución internacional de ciberdelitos.

INTRODUCCIÓN

Hasta la clase anterior analizamos protección de datos personales, privacidad y responsabilidad derivada del tratamiento de información.

Hoy vamos a avanzar un paso más y estudiar qué sucede cuando la tecnología deja de ser una herramienta y pasa a convertirse en el medio para cometer un delito.

La pregunta que atravesará toda la clase será:

¿Cómo demuestra la Justicia un delito que ocurrió dentro de una computadora o a través de Internet?

Para responderla necesitaremos combinar conocimientos jurídicos con conceptos propios de la informática.

Novedad tecnológica

Durante los últimos meses crecieron exponencialmente las estafas realizadas mediante inteligencia artificial.

Hoy existen programas capaces de clonar la voz de una persona con apenas algunos segundos de audio.

También pueden generar videos falsos (deepfakes) extremadamente convincentes.

Esto plantea un enorme desafío:

Si una grabación puede ser fabricada, ¿cómo demuestra un juez que una prueba digital es auténtica?

La respuesta está en la evidencia digital, la pericia informática y la cadena de custodia.

Ese será uno de los ejes de nuestra clase.

BLOQUE I

¿QUÉ ES UN DELITO INFORMÁTICO?

Comenzaremos la clase con una pregunta sencilla:

> **¿Todo delito cometido utilizando una computadora o Internet es un delito informático?**

La respuesta es **no**.

Esta es una de las primeras confusiones que suelen aparecer cuando hablamos de ciberdelincuencia.

Muchas personas creen que cualquier conducta ilícita realizada mediante una computadora constituye un delito informático. Sin embargo, desde el punto de vista jurídico, esto no es correcto.

Concepto de delito informático

En nuestro ordenamiento jurídico no existe una definición única y expresa de "delito informático".

La doctrina ha elaborado distintas definiciones, pero en términos generales podemos afirmar que son aquellos delitos en los cuales:

- la informática, los sistemas o los datos constituyen el objeto directamente protegido por la ley penal; o
- las tecnologías de la información y las comunicaciones son utilizadas como instrumento esencial para cometer el ilícito.

En otras palabras, la tecnología puede ocupar dos posiciones diferentes:

- puede ser **la víctima del ataque**, cuando el bien jurídico afectado es un sistema, una base de datos o la información almacenada en ella; o

- puede ser **la herramienta utilizada por el delincuente**, facilitando la comisión de una conducta prohibida.

Por ello, la informática puede ser tanto el objeto como el medio del delito.

Delitos tradicionales y delitos informáticos

Es importante distinguir entre un delito tradicional cometido por medios digitales y un verdadero delito informático.

La simple utilización de Internet o de un dispositivo electrónico no modifica necesariamente la naturaleza jurídica del delito.

Por ejemplo, si una persona envía una amenaza mediante WhatsApp, correo electrónico o Telegram, continúa cometiendo el delito de amenazas previsto en el Código Penal.

El medio tecnológico cambia, pero la conducta típica sigue siendo exactamente la misma.

Del mismo modo, una injuria publicada en una red social continúa siendo una lesión al honor; una estafa realizada por mensaje de texto continúa siendo una estafa; una extorsión realizada por correo electrónico sigue siendo una extorsión.

La tecnología únicamente reemplaza el medio tradicional de comunicación.

En cambio, existen conductas que solo pueden comprenderse a partir de la existencia de sistemas informáticos.

Por ejemplo:

- ingresar sin autorización a un servidor protegido;
- alterar una base de datos;
- manipular un sistema bancario para modificar una transferencia;
- instalar un ransomware que cifra toda la información de una empresa.

En estos supuestos, el componente tecnológico resulta esencial para la configuración del ilícito.

La informática como objeto protegido

En algunos delitos, el Derecho protege directamente la confidencialidad, la integridad o la disponibilidad de la información.

Pensemos en una empresa que almacena los datos personales de miles de clientes.

Si un atacante accede ilegalmente a esa base de datos, el perjuicio no consiste únicamente en el ingreso no autorizado, sino también en la afectación de la confidencialidad de la información.

Si además modifica o elimina registros, también se compromete la integridad de los datos.

Y si bloquea completamente el acceso mediante un ransomware, afecta la disponibilidad del sistema.

Estos tres conceptos constituyen la denominada **tríada CIA (Confidentiality, Integrity and Availability)**, uno de los pilares fundamentales de la seguridad informática.

Observarán que muchas figuras penales incorporadas por la Ley 26.388 protegen precisamente alguno de estos tres valores.

La informática como medio para cometer un delito

En otras situaciones, la informática no es el bien jurídico protegido sino el instrumento utilizado para producir un daño patrimonial o afectar otros derechos.

Por ejemplo, un delincuente obtiene mediante phishing las credenciales bancarias de una víctima.

Luego ingresa a su home banking y modifica el destinatario de una transferencia para apropiarse del dinero.

En este caso, el sistema informático es el medio empleado para producir un perjuicio económico.

La manipulación tecnológica se convierte en el mecanismo utilizado para cometer el fraude.

Ejemplos comparativos

Analicemos algunos supuestos.

Caso 1

Una persona envía por WhatsApp el mensaje:

"Si mañana declarás en el juicio, te voy a lastimar."

¿Qué delito observamos?

Nos encontramos frente a una amenaza.

El hecho de utilizar una aplicación de mensajería instantánea no transforma la conducta en un delito informático.

La tecnología funciona únicamente como canal de comunicación.

Caso 2

Un empleado ingresa utilizando credenciales ajenas al servidor de su empresa y descarga la base de datos de clientes.

Aquí sí aparece una figura específicamente vinculada con los sistemas informáticos.

La conducta puede encuadrarse como acceso ilegítimo, ya que el ingreso se produce sin autorización sobre un sistema protegido.

Caso 3

Un atacante modifica el número de CBU registrado en un sistema contable para que los pagos de proveedores se acrediten en su propia cuenta bancaria.

Este supuesto constituye un claro ejemplo de fraude informático.

El perjuicio patrimonial se produce mediante la manipulación de un sistema de información.

Caso 4

Un hacker instala un ransomware que cifra todos los servidores de un hospital e impide el acceso a las historias clínicas.

En este caso se afecta la disponibilidad de la información y la integridad del sistema, configurándose un supuesto de daño informático.

Pregunta para el debate

Supongamos que una persona publica en una red social una grave calumnia contra otra.

¿Estamos frente a un delito informático o frente a un delito tradicional cometido mediante una plataforma digital?

La respuesta correcta es que se trata de un delito tradicional cuya ejecución se realiza utilizando un medio tecnológico.

Esta distinción resulta fundamental porque permite identificar correctamente cuál es el tipo penal aplicable y cuál es el bien jurídico protegido.

Idea central para recordar

Al estudiar delitos informáticos no debemos preguntarnos solamente **qué tecnología se utilizó**, sino **qué conducta realizó el autor y qué bien jurídico fue afectado**.

El Derecho Penal no castiga computadoras, programas o redes.

Lo que sanciona son conductas humanas que lesionan bienes jurídicos protegidos, aunque esas conductas hoy se desarrollen cada vez más dentro de entornos digitales.

Bien jurídico protegido

El Derecho Penal protege determinados intereses sociales.

Cada delito protege un bien jurídico diferente.

Delito	Bien jurídico protegido
Acceso ilegítimo	Confidencialidad
Interceptación	Secreto de las comunicaciones
Daño informático	Integridad y disponibilidad
Fraude informático	Patrimonio
Grooming	Integridad sexual del menor

Comprender qué bien jurídico se protege ayuda a interpretar correctamente cada figura penal.

BLOQUE II

LA TRÍADA CIA Y SU RELACIÓN CON EL DERECHO

Introducción

Para comprender verdaderamente los delitos informáticos, es necesario incorporar un concepto fundamental de la seguridad informática: la **tríada CIA**.

Aunque se trata de un modelo desarrollado desde la informática y la ciberseguridad, sus principios tienen una estrecha relación con los bienes jurídicos que protege el Derecho Penal.

De hecho, muchas de las figuras incorporadas por la Ley 26.388 buscan sancionar conductas que lesionan alguno de estos tres pilares esenciales de la información.

Por ello, podemos afirmar que **la ciberseguridad y el Derecho Penal persiguen un mismo objetivo: proteger la información y los sistemas informáticos, aunque lo hagan mediante herramientas diferentes**.

Mientras la informática intenta prevenir el ataque mediante controles técnicos, el Derecho busca sancionar las conductas ilícitas cuando esos controles son vulnerados.

¿Qué significa CIA?

CIA es el acrónimo de tres palabras en inglés:

- **C – Confidentiality (Confidencialidad)**
- **I – Integrity (Integridad)**

- **A – Availability (Disponibilidad)**

Estos tres principios constituyen la base de cualquier política moderna de seguridad informática.

Cuando alguno de ellos resulta afectado, puede producirse un incidente de seguridad e incluso configurarse un delito.

Veamos cada uno de ellos.

1.CONFIDENCIALIDAD (CONFIDENTIALITY)

Concepto

La confidencialidad implica que la información solo pueda ser conocida por las personas autorizadas para acceder a ella.

Su finalidad es impedir que terceros no autorizados conozcan datos privados, estratégicos o sensibles.

En otras palabras, protege el secreto de la información.

Ejemplo cotidiano

Pensemos en la historia clínica digital de un paciente.

Solo deberían acceder:

- el propio paciente;
- su médico tratante;
- el personal autorizado.

Si cualquier empleado del hospital pudiera consultar esa información, la confidencialidad estaría completamente vulnerada.

Ejemplo informático

Un atacante obtiene las credenciales de administrador de una empresa e ingresa al servidor donde se almacenan los datos de miles de clientes.

Aunque no modifique absolutamente nada, el solo acceso indebido afecta la confidencialidad de la información.

Por ese motivo, el Código Penal sanciona el acceso ilegítimo a sistemas protegidos.

Relación con el Derecho

Desde la perspectiva jurídica, la confidencialidad protege derechos fundamentales como:

- la privacidad;
- la intimidad;
- el secreto de las comunicaciones;
- la protección de datos personales.

Por ello, cuando alguien accede sin autorización a una base de datos o intercepta comunicaciones privadas, no solo vulnera un sistema informático, sino también derechos constitucionalmente protegidos.

Pregunta para los alumnos

Si un empleado tiene la contraseña de su jefe porque este se la compartió hace un año y hoy ingresa sin permiso para consultar información confidencial,

¿el problema es técnico, jurídico o ambos?

La respuesta es que es **ambos**.

Técnicamente logró autenticarse.

Jurídicamente carece de autorización para acceder.

Este ejemplo demuestra que **autenticación y autorización son conceptos distintos**.

---

2. INTEGRIDAD (INTEGRITY)

Concepto

La integridad garantiza que la información permanezca correcta, completa y libre de modificaciones no autorizadas.

No basta con que los datos existan.

También deben mantenerse exactamente como fueron creados o modificados por quienes tienen facultades para hacerlo.

La integridad asegura que la información sea confiable.

Ejemplo cotidiano

Supongamos que un estudiante aprueba una materia con nota ocho.

Si alguien modifica ilegalmente el sistema académico y cambia esa nota por un dos, la información sigue existiendo, pero ya no es correcta.

La integridad del registro fue alterada.

Ejemplo informático

Un atacante accede a una base de datos bancaria y modifica los saldos de determinadas cuentas.

Aunque el sistema continúe funcionando normalmente, la información ha sido alterada.

La lesión principal recae sobre la integridad de los datos.

Relación con el Derecho

Muchas figuras penales protegen precisamente este aspecto.

Modificar registros contables.

Alterar historias clínicas.

Cambiar beneficiarios de una transferencia bancaria.

Manipular expedientes electrónicos.

Todas estas conductas afectan la integridad de la información y pueden producir importantes consecuencias jurídicas y patrimoniales.

Caso práctico

Una persona ingresa al sistema de una universidad y modifica las calificaciones de varios alumnos.

¿Qué ocurrió?

No desapareció la información.

No se bloqueó el sistema.

Lo que se alteró fue la autenticidad y confiabilidad de los datos almacenados.

Por ello, el bien jurídico lesionado es la integridad.

---

3. DISPONIBILIDAD (AVAILABILITY)

Concepto

La disponibilidad garantiza que la información y los sistemas puedan ser utilizados por quienes están autorizados cuando lo necesiten.

Un dato perfectamente protegido carece de utilidad si nadie puede acceder a él.

La disponibilidad resulta especialmente importante en servicios críticos.

Ejemplo cotidiano

Pensemos en un hospital.

Los médicos necesitan acceder a las historias clínicas en forma inmediata.

Si el sistema permanece caído durante varias horas, la atención médica puede verse gravemente afectada.

Aunque la información no haya sido robada ni modificada, su falta de disponibilidad genera un enorme perjuicio.

Ejemplo informático

Uno de los ejemplos más conocidos es el ransomware.

Este tipo de malware cifra todos los archivos de una organización e impide acceder a ellos hasta que se pague un rescate.

Los datos siguen almacenados.

No fueron destruidos.

Sin embargo, los usuarios autorizados no pueden utilizarlos.

Por ello, el ataque afecta principalmente la disponibilidad de la información.

Relación con el Derecho

La destrucción o inutilización de datos y sistemas puede configurar delitos previstos por el Código Penal.

La afectación de la disponibilidad puede generar, además, importantes responsabilidades civiles por los daños ocasionados a clientes, usuarios o terceros.

La tríada CIA aplicada a casos reales

Veamos algunos ejemplos.

Caso 1

Un hacker ingresa sin autorización a la base de datos de una empresa y observa toda la información sin modificar ningún registro.

¿Qué principio resulta afectado?

Confidencialidad.

Porque personas no autorizadas accedieron a información reservada.

Caso 2

Un empleado modifica el número de cuenta bancaria de un proveedor antes de realizar un pago.

¿Qué principio se vulnera?

Integridad.

Porque la información fue alterada de manera indebida.

Caso 3

Un ransomware cifra todos los servidores de una clínica e impide acceder a las historias clínicas.

¿Qué principio resulta principalmente afectado?

Disponibilidad.

Porque la información existe, pero no puede utilizarse.

Caso 4

Un atacante ingresa a un sistema, descarga información confidencial y luego elimina toda la base de datos.

¿Qué principios fueron afectados?

En este supuesto se lesionan simultáneamente:

- la **confidencialidad**, porque accedió indebidamente a la información;
- la **integridad**, porque modificó o destruyó los datos;
- la **disponibilidad**, porque el sistema dejó de prestar su función.

Es un claro ejemplo de un ataque que compromete toda la tríada CIA.

La visión de la informática y la visión del Derecho

Desde la informática, la pregunta suele ser:

¿Qué medida técnica implementamos para evitar este incidente?

Las respuestas pueden ser:

- autenticación multifactor;
- cifrado;
- control de accesos;
- firewalls;
- backups;
- monitoreo de eventos;
- segmentación de redes.

Desde el Derecho, en cambio, la pregunta es diferente:

¿Qué conducta realizó la persona y qué bien jurídico lesionó?

El Derecho no sanciona fallas técnicas.

Sanciona conductas humanas que afectan derechos protegidos por la ley.

Por ello, ambas disciplinas son complementarias.

La ciberseguridad busca prevenir.

El Derecho Penal busca investigar, juzgar y sancionar cuando la prevención ha fracasado.

Actividad para el aula

Analicen los siguientes supuestos e indiquen cuál de los tres principios de la tríada CIA resulta principalmente afectado.

Caso A

Un empleado accede sin autorización a los sueldos de todos los trabajadores.

Caso B

Un desarrollador modifica deliberadamente el código fuente de una aplicación para generar errores en producción.

Caso C

Un ataque de ransomware impide durante tres días el funcionamiento del sistema informático de una municipalidad.

Caso D

Un ciberdelincuente descarga una base de datos y luego elimina todos los registros almacenados.

Luego del análisis, discutan si en alguno de los casos se afectan simultáneamente más de uno de los pilares de la tríada.

Conclusión

La tríada CIA constituye uno de los conceptos más importantes de la seguridad informática moderna.

Comprenderla permite interpretar con mayor claridad los delitos informáticos incorporados por nuestra legislación.

Cada ataque informático puede analizarse identificando cuál de estos principios fue vulnerado y qué bien jurídico protege el Derecho.

Por eso, al estudiar delitos informáticos no debemos pensar únicamente en computadoras o redes, sino en **la protección jurídica de la confidencialidad, la integridad y la disponibilidad de la información**, pilares esenciales para el funcionamiento de la sociedad digital actual.

BLOQUE III

LA LEY 26.388 Y LA MODERNIZACIÓN DEL CÓDIGO PENAL ARGENTINO

Introducción

Hasta hace poco más de veinte años, gran parte de los delitos previstos por el Código Penal argentino habían sido pensados para una realidad completamente diferente a la actual.

Cuando se sancionó el Código Penal, no existían Internet, las redes sociales, la banca electrónica, el comercio electrónico ni las bases de datos masivas.

Sin embargo, el desarrollo tecnológico transformó profundamente la forma en que las personas trabajan, se comunican y realizan operaciones económicas.

Como consecuencia de ello, también aparecieron nuevas modalidades delictivas que el derecho debía regular.

Frente a esta realidad, el Estado argentino sancionó la **Ley 26.388**, publicada en el año 2008, mediante la cual se modificó el Código Penal para incorporar figuras específicas vinculadas con las tecnologías de la información y las comunicaciones.

El objetivo de esta reforma fue brindar protección penal frente a conductas que afectan sistemas informáticos, datos digitales y comunicaciones electrónicas.

No se creó un nuevo Código Penal informático, sino que se adaptaron distintas figuras ya existentes e incorporaron nuevos tipos penales adecuados a la sociedad digital.

¿Por qué fue necesaria esta reforma?

Pensemos en una situación sencilla.

Hace treinta años, para obtener información confidencial era necesario ingresar físicamente a una oficina y sustraer documentos en papel.

Hoy, un atacante puede acceder desde otro continente a un servidor y descargar millones de registros en pocos minutos.

El daño potencial es mucho mayor y la forma de comisión completamente distinta.

El Derecho debía adaptarse a esta nueva realidad tecnológica.

Por ello, la Ley 26.388 incorporó figuras destinadas a proteger:

- la privacidad;
- las comunicaciones electrónicas;
- los sistemas informáticos;
- las bases de datos;
- el patrimonio cuando resulta afectado mediante manipulación tecnológica.

ACCESO ILEGÍTIMO

Artículo 153 bis del Código Penal

Concepto

Una de las figuras más importantes incorporadas por la reforma es el delito de **acceso ilegítimo**.

Consiste en ingresar, sin autorización, a un sistema informático o a una base de datos de acceso restringido o protegida.

El aspecto fundamental de esta figura no es la dificultad técnica del acceso.

Tampoco importa si fue necesario vulnerar sofisticados mecanismos de seguridad.

Lo verdaderamente relevante es la existencia o no de autorización para ingresar.

Por ello, el bien jurídico protegido es la confidencialidad de la información y la inviolabilidad de los sistemas protegidos.

El concepto clave: autorización

Para los futuros programadores, administradores de sistemas y desarrolladores de software, este concepto resulta esencial.

Muchas veces se confunden dos términos que poseen significados completamente diferentes:

Autenticación

Consiste en demostrar quién es el usuario.

Es el proceso mediante el cual un sistema verifica la identidad de quien intenta acceder.

Ejemplos:

- ingresar usuario y contraseña;
- utilizar autenticación biométrica;
- autenticación multifactor;
- certificados digitales.

La autenticación responde a la pregunta:

¿Quién sos?

Autorización

La autorización determina qué acciones puede realizar un usuario una vez autenticado.

Responde a la pregunta:

¿Qué tenés permitido hacer?

Un usuario puede identificarse correctamente y, sin embargo, no estar autorizado para acceder a determinada información.

Ejemplo práctico

Imaginemos un hospital.

Un médico inicia sesión correctamente utilizando su usuario y contraseña.

El sistema verifica su identidad.

La autenticación fue exitosa.

Sin embargo, intenta acceder a las historias clínicas de pacientes pertenecientes a otro servicio para el cual no posee permisos.

Aunque el sistema reconozca quién es, no está autorizado para consultar esa información.

La autenticación existe.

La autorización no.

Autenticación no significa autorización

Esta diferencia es una de las más importantes en materia de delitos informáticos.

Una contraseña válida no convierte automáticamente un acceso en legítimo.

Una persona puede conocer perfectamente una contraseña y, aun así, carecer de autorización jurídica para utilizarla.

Por ello, el eje del artículo 153 bis no es la contraseña, sino el consentimiento válido para ingresar al sistema.

Caso práctico

Un desarrollador participa durante años en la creación de un sistema de gestión empresarial.

Mientras trabaja en la empresa posee privilegios de administrador.

Meses después presenta su renuncia.

La empresa omite eliminar su usuario.

Tiempo después decide ingresar nuevamente al servidor utilizando sus antiguas credenciales.

No vulneró ninguna medida técnica.

No hackeó el sistema.

No rompió una contraseña.

Simplemente utilizó un usuario que aún funcionaba.

¿Existe acceso ilegítimo?

Desde la perspectiva jurídica, sí puede configurarse este delito, porque el vínculo laboral terminó y con él cesó la autorización para ingresar al sistema.

El acceso es técnicamente válido pero jurídicamente ilegítimo.

Otros ejemplos

- utilizar la contraseña de un compañero de trabajo;
- ingresar al panel de administración aprovechando credenciales olvidadas;
- acceder a una base de datos luego de finalizar un contrato;
- utilizar una sesión abierta por otro usuario sin autorización.

En todos estos casos, el elemento central es la ausencia de autorización.

INTERCEPTACIÓN DE COMUNICACIONES

Artículo 153 del Código Penal

Concepto

Otra figura relevante protege el secreto de las comunicaciones privadas.

Toda persona tiene derecho a comunicarse sin que terceros intercepten, lean o capturen esas comunicaciones.

Este derecho deriva del principio constitucional de privacidad y del secreto de la correspondencia.

La protección alcanza tanto a comunicaciones tradicionales como electrónicas.

¿Qué significa interceptar?

Interceptar implica captar una comunicación durante su transmisión o acceder indebidamente a su contenido.

No es necesario alterar el mensaje.

Basta con obtener acceso a una comunicación que debía permanecer reservada.

Ejemplos

- instalar un software espía para leer correos electrónicos;
- capturar tráfico de red mediante herramientas de sniffing;
- acceder ilegalmente a una cuenta de correo;
- interceptar mensajes enviados mediante aplicaciones de mensajería instantánea;
- instalar malware destinado a registrar conversaciones.

¿Qué protege esta figura?

No solamente protege el contenido del mensaje.

También protege la privacidad del acto comunicacional.

Las personas deben poder comunicarse libremente sin temor a ser observadas o vigiladas por terceros.

Caso práctico

Una empresa instala clandestinamente un software que registra todas las conversaciones privadas que sus empleados mantienen desde sus cuentas personales durante el horario laboral.

Más allá de las cuestiones laborales, la conducta puede afectar el secreto de las comunicaciones y la privacidad de los trabajadores.

DAÑO INFORMÁTICO

Artículo 183 del Código Penal

Concepto

El daño informático consiste en destruir, alterar, inutilizar o hacer inaccesibles datos, programas o sistemas informáticos.

En este caso, el bien jurídico protegido es principalmente la integridad y la disponibilidad de la información.

Ejemplos clásicos

- eliminar una base de datos;
- modificar registros críticos;
- destruir archivos esenciales;
- borrar respaldos;
- alterar configuraciones de servidores;
- inutilizar sistemas mediante malware.

El ransomware como ejemplo actual

Uno de los ataques más frecuentes en la actualidad es el ransomware.

Este tipo de software malicioso cifra los archivos de una organización e impide su utilización.

El atacante exige luego el pago de un rescate para proporcionar la clave de descifrado.

Sin embargo, la modalidad delictiva evolucionó considerablemente.

Hoy muchos grupos criminales implementan la denominada **doble extorsión**.

Primero roban la información.

Luego cifran los servidores.

Finalmente amenazan con publicar los datos obtenidos si la víctima no paga.

Por ello, el ataque afecta simultáneamente:

- la confidencialidad;
- la integridad;
- la disponibilidad.

Caso práctico

Una empresa descubre que todas sus computadoras muestran un mensaje indicando que sus archivos fueron cifrados y exigiendo el pago de una suma en criptomonedas.

Los sistemas dejan de funcionar durante varios días.

Aunque la información continúe almacenada, resulta inaccesible.

Se ha lesionado gravemente la disponibilidad de los datos.

FRAUDE INFORMÁTICO

Artículo 173 inciso 16 del Código Penal

Concepto

Existe fraude informático cuando una persona obtiene un beneficio económico indebido mediante la manipulación de un sistema informático o de los datos contenidos en él.

Aquí el bien jurídico protegido es el patrimonio.

La informática constituye el medio utilizado para producir el perjuicio económico.

Ejemplos

- modificar una transferencia bancaria;
- alterar saldos de cuentas;
- cambiar el CBU registrado para recibir un pago;
- modificar registros contables;
- alterar órdenes de pago;
- manipular sistemas de facturación.

El phishing y el fraude

Muchas estafas comienzan con un correo electrónico falso o un sitio web fraudulento destinado a obtener credenciales.

Esta técnica se conoce como phishing.

Sin embargo, desde la perspectiva penal, la obtención de las credenciales suele constituir solo la primera etapa del ataque.

El fraude se perfecciona cuando el delincuente utiliza esa información para manipular el sistema y provocar un perjuicio económico.

Caso práctico

Un atacante envía un correo falso simulando ser una entidad bancaria.

La víctima ingresa sus credenciales.

Con esos datos, el delincuente accede al home banking y modifica el destinatario de una transferencia por un alias bajo su control.

Finalmente el dinero es transferido.

La manipulación del sistema produce un beneficio patrimonial indebido y configura un supuesto de fraude informático.

GROOMING

Artículo 131 del Código Penal

Concepto

El grooming consiste en contactar a una persona menor de edad mediante medios digitales con fines sexuales.

La conducta puede realizarse a través de:

- redes sociales;
- videojuegos en línea;
- aplicaciones de mensajería;
- plataformas educativas;
- cualquier otro medio electrónico.

Características

No requiere un encuentro físico.

No exige que exista un abuso sexual consumado.

El delito se configura por el acercamiento al menor con una finalidad sexual.

La ley busca intervenir de manera preventiva para proteger la integridad de niños, niñas y adolescentes.

Etapas habituales del grooming

En muchos casos el agresor:

1. crea una identidad falsa;
2. establece una relación de confianza;
3. obtiene información personal;
4. solicita imágenes íntimas;
5. amenaza o manipula emocionalmente a la víctima.

Este proceso puede extenderse durante semanas o meses.

Caso práctico

Un adulto crea un perfil falso haciéndose pasar por un adolescente.

Comienza a conversar diariamente con una niña de trece años a través de una red social.

Con el paso del tiempo intenta obtener fotografías íntimas y propone un encuentro personal.

Aunque nunca llegue a concretarse la reunión, la conducta puede configurar grooming, porque el delito se consuma con el contacto digital realizado con finalidad sexual.

Reflexión final del bloque

La Ley 26.388 representó un paso fundamental en la modernización del Derecho Penal argentino.

Gracias a esta reforma, el ordenamiento jurídico incorporó herramientas para responder a nuevas modalidades delictivas surgidas en el entorno digital.

Sin embargo, el verdadero desafío no consiste únicamente en conocer los artículos del Código Penal.

Para un profesional de la programación resulta mucho más importante comprender **qué conducta se sanciona, qué bien jurídico protege la ley y qué evidencia técnica permitirá demostrar el hecho ante un tribunal**.

En definitiva, detrás de cada delito informático existe una interacción permanente entre tecnología y derecho: la informática explica cómo ocurrió el ataque y el Derecho determina sus consecuencias jurídicas.

ACTIVIDAD 1

Clasifiquen el siguiente caso.

Un empleado utiliza la contraseña de un compañero para ingresar al sistema de Recursos Humanos y descargar los salarios de toda la empresa.

Preguntas:

- ¿Qué delito observan?
- ¿Qué bien jurídico resulta afectado?
- ¿Qué evidencia digital solicitarían?

BLOQUE IV

LA EVIDENCIA DIGITAL Y SU IMPORTANCIA EN EL PROCESO PENAL

Introducción

En todo proceso judicial, uno de los principios fundamentales es que **los hechos deben ser probados**.

No basta con afirmar que un delito ocurrió.

Es necesario demostrarlo mediante elementos objetivos que permitan reconstruir lo sucedido y convencer al juez sobre la existencia del hecho y la responsabilidad de sus autores.

En el ámbito de los delitos informáticos, esta tarea presenta una dificultad particular: muchas de las pruebas no son físicas, sino digitales.

A diferencia de un arma, un documento en papel o una huella dactilar, la evidencia informática puede copiarse, modificarse o eliminarse con enorme facilidad.

Por ello, su correcta obtención y preservación resultan esenciales para el éxito de cualquier investigación penal.

En muchas oportunidades, **un solo registro de acceso o un archivo de log correctamente preservado puede ser más valioso que decenas de testimonios**.

¿Qué es la evidencia digital?

La evidencia digital es toda información almacenada o transmitida en formato electrónico que posee valor para demostrar un hecho dentro de un proceso judicial.

Su función es permitir reconstruir los acontecimientos ocurridos, identificar responsables y verificar la autenticidad de determinadas acciones.

La evidencia digital constituye hoy uno de los principales medios probatorios en investigaciones relacionadas con ciberdelitos, fraudes electrónicos, accesos ilegítimos y ataques informáticos.

Sin embargo, también resulta fundamental en investigaciones por delitos tradicionales, ya que gran parte de nuestras actividades cotidianas dejan rastros digitales.

¿Dónde puede encontrarse evidencia digital?

La información útil para una investigación puede provenir de múltiples fuentes.

Entre las más importantes encontramos:

- registros de eventos o **logs**;
- correos electrónicos;
- conversaciones mantenidas por aplicaciones de mensajería;
- metadatos de documentos o imágenes;
- copias de seguridad o **backups**;
- direcciones IP;
- registros de autenticación;
- auditorías de sistemas;
- archivos de configuración;
- historiales de navegación;
- dispositivos móviles;
- servidores;
- bases de datos;
- servicios en la nube.

Cada uno de estos elementos aporta una parte de la historia.

La investigación consiste en correlacionarlos para reconstruir cronológicamente los hechos.

Los logs: la memoria de un sistema

Uno de los elementos más importantes en informática forense son los **logs**.

Un log es un registro automático generado por un sistema informático que documenta las actividades realizadas.

Podría compararse con la "caja negra" de un avión.

Cuando ocurre un incidente, los logs permiten conocer qué sucedió y en qué momento.

¿Qué información contienen?

Dependiendo del sistema, un log puede registrar:

- fecha y hora de acceso;
- usuario autenticado;
- dirección IP utilizada;
- dispositivo empleado;
- operaciones realizadas;
- errores del sistema;
- modificaciones efectuadas;
- intentos fallidos de autenticación;
- privilegios utilizados.

Estos registros permiten reconstruir con gran precisión una secuencia de acontecimientos.

Ejemplo práctico

Supongamos que una empresa detecta que se modificó ilegalmente el número de cuenta bancaria de un proveedor.

Los logs pueden indicar:

- qué usuario realizó el cambio;
- desde qué computadora se efectuó;
- a qué hora ocurrió;
- qué dirección IP fue utilizada;
- qué otras operaciones se realizaron durante la misma sesión.

Toda esta información puede resultar determinante para la investigación.

Correos electrónicos y mensajería

Los correos electrónicos constituyen otra fuente frecuente de evidencia.

No solamente interesa el contenido del mensaje.

También poseen enorme importancia sus datos técnicos.

Entre ellos:

- dirección del remitente;
- destinatarios;
- fecha y hora exactas;
- servidores intervinientes;
- encabezados técnicos (*headers*);
- archivos adjuntos;
- firmas digitales.

Los encabezados permiten reconstruir el recorrido que siguió un correo y detectar posibles falsificaciones.

De manera similar, las aplicaciones de mensajería pueden aportar conversaciones, horarios de envío, identificadores de dispositivos y otra información relevante.

Metadatos: información oculta

Los metadatos son datos que describen otros datos.

Aunque muchas veces pasan inadvertidos, poseen enorme valor probatorio.

Por ejemplo, una fotografía puede contener información relativa a:

- fecha de creación;
- dispositivo utilizado;
- ubicación geográfica;
- modelo de cámara;
- programa con el que fue editada.

Un documento digital puede indicar:

- autor;
- fecha de creación;
- fecha de modificación;
- usuario que realizó cambios;
- software empleado.

Estos elementos permiten verificar autenticidad o detectar manipulaciones.

Backups o copias de seguridad

Los respaldos constituyen una herramienta esencial tanto para la continuidad operativa como para la investigación.

Permiten recuperar información eliminada y comparar versiones anteriores de archivos o bases de datos.

En numerosos casos de ransomware, los backups representan la única posibilidad de restaurar la actividad de una organización.

Asimismo, pueden demostrar cómo se encontraba un sistema antes de sufrir un ataque.

Registros de autenticación y auditoría

Todo sistema moderno registra quién ingresó, cuándo lo hizo y qué acciones ejecutó.

Estos registros permiten verificar:

- inicios de sesión;
- cierres de sesión;
- cambios de contraseña;
- asignación de permisos;
- modificaciones críticas;
- eliminación de archivos;
- acceso a bases de datos.

Desde el punto de vista jurídico, estos registros permiten vincular una conducta con un usuario determinado, aunque luego será necesario determinar quién utilizó realmente esa cuenta.

La reconstrucción de los hechos

La investigación informática se asemeja al armado de un rompecabezas.

Ninguna evidencia aislada suele ser suficiente.

El investigador debe relacionar múltiples fuentes de información para reconstruir la secuencia completa de acontecimientos.

Por ejemplo:

- un log registra un acceso;
- una dirección IP identifica una conexión;
- una cámara muestra quién utilizaba el equipo;
- un correo electrónico acredita la autorización o su ausencia;
- un registro de auditoría demuestra las modificaciones realizadas.

La combinación de todas estas pruebas permite elaborar una reconstrucción confiable del hecho investigado.

La cadena de custodia

Concepto

Una vez obtenida la evidencia, surge un nuevo desafío: garantizar que permanezca inalterada.

Para ello existe la **cadena de custodia**.

Se trata del conjunto de procedimientos destinados a asegurar la autenticidad e integridad de la evidencia desde su obtención hasta su presentación en juicio.

Su finalidad consiste en demostrar que la prueba analizada por el juez es exactamente la misma que fue obtenida durante la investigación.

¿Por qué es tan importante?

La evidencia digital puede modificarse en pocos segundos.

Si no existe un adecuado control sobre su preservación, cualquier parte podría sostener que fue alterada o manipulada.

Una cadena de custodia deficiente puede disminuir considerablemente el valor probatorio de una evidencia o incluso determinar su exclusión del proceso.

¿Qué debe documentarse?

Como mínimo debe registrarse:

- quién obtuvo la evidencia;
- fecha y hora de obtención;
- lugar donde fue encontrada;
- procedimiento utilizado para su recolección;
- forma de preservación;
- soporte utilizado para almacenarla;
- personas que tuvieron contacto con ella;
- traslados realizados;
- análisis efectuados;
- identidad del perito que intervino.

Cada movimiento debe quedar documentado.

La trazabilidad constituye la esencia de la cadena de custodia.

Ejemplo práctico

Durante un allanamiento se secuestra una computadora.

El funcionario policial debe registrar:

- el lugar exacto donde fue hallada;
- la fecha y hora del secuestro;
- el estado en que se encontraba;
- quién la recibió;
- cómo fue transportada;
- dónde quedó almacenada;
- quién realizó posteriormente el análisis pericial.

Si alguno de estos pasos no queda documentado, la defensa podría cuestionar la autenticidad de la prueba.

La pericia informática

Concepto

El perito informático es el profesional especializado encargado de analizar técnicamente la evidencia digital.

Su misión consiste en aplicar conocimientos científicos para responder preguntas relevantes para el proceso judicial.

En otras palabras, traduce información altamente técnica en conclusiones comprensibles para el juez.

Funciones principales

Entre sus tareas más frecuentes se encuentran:

- recuperar archivos eliminados;
- reconstruir cronologías de eventos;
- analizar programas maliciosos;
- verificar la integridad de archivos;
- identificar modificaciones realizadas;
- detectar accesos indebidos;
- correlacionar registros provenientes de distintas fuentes;
- analizar dispositivos electrónicos;
- reconstruir actividades desarrolladas por un usuario.

Su informe constituye un elemento de enorme importancia dentro del proceso penal.

Caso práctico

Una empresa denuncia un ataque informático.

El perito analiza los servidores y determina que:

- el acceso ocurrió a las 02:17 horas;

- se utilizó una cuenta administrativa;
- previamente se había ejecutado un archivo malicioso recibido por correo electrónico;
- posteriormente se eliminaron registros y se cifraron los servidores.

A partir de estos datos puede reconstruirse técnicamente la secuencia del ataque.

¿Una dirección IP identifica automáticamente al autor?

Esta es una de las preguntas más frecuentes en materia de ciberdelitos.

La respuesta es **no**.

Una dirección IP identifica una conexión a Internet en un determinado momento, pero **no identifica por sí sola a la persona que realizó una conducta**.

Por ello, nunca debe confundirse una conexión con una autoría.

¿Por qué una IP no alcanza?

Existen múltiples razones.

NAT

En muchos hogares y empresas varios dispositivos comparten una única dirección IP pública.

Por ello, la IP identifica la red, pero no determina cuál de los equipos realizó la acción.

VPN

Las redes privadas virtuales permiten que la conexión aparezca como proveniente de otro lugar del mundo.

Un usuario ubicado en Argentina puede aparecer conectado desde otro país.

Redes compartidas

Universidades, hoteles, aeropuertos o cafeterías ofrecen conexiones utilizadas simultáneamente por numerosas personas.

La IP identifica el punto de acceso, pero no individualiza al usuario.

Equipos comprometidos

Un atacante puede controlar remotamente una computadora ajena infectada con malware y utilizarla para cometer delitos.

En ese caso, la IP corresponderá a la víctima y no al verdadero autor.

Proxies y servicios de anonimización

Diversos servicios intermedian entre el usuario e Internet ocultando su dirección real.

Esto dificulta considerablemente la atribución de responsabilidad.

La atribución de autoría

Por estas razones, la investigación penal nunca debe basarse exclusivamente en una dirección IP.

La autoría surge de la valoración conjunta de múltiples elementos probatorios.

Entre ellos pueden encontrarse:

- registros de autenticación;
- cámaras de seguridad;
- geolocalización;
- dispositivos secuestrados;
- historial de navegación;
- registros telefónicos;
- pericias informáticas;
- declaraciones testimoniales;
- evidencia documental.

Solo el análisis integral de todos estos elementos permite alcanzar una conclusión razonablemente fundada sobre la identidad del responsable.

Actividad para el aula

Analicen el siguiente supuesto.

Una empresa detecta una transferencia bancaria fraudulenta.

Los registros muestran que la operación fue realizada desde una dirección IP perteneciente a la propia organización.

Respondan:

1. ¿Puede afirmarse automáticamente quién fue el autor?
2. ¿Qué otras evidencias solicitarían para reconstruir los hechos?
3. ¿Qué importancia tendría la existencia de registros de autenticación y cámaras de seguridad?
4. ¿Cómo influiría una adecuada cadena de custodia en un eventual proceso judicial?

Conclusión

En los delitos informáticos, la evidencia digital constituye el elemento central de toda investigación.

Sin registros confiables, correctamente preservados y analizados mediante procedimientos técnicos adecuados, resulta extremadamente difícil reconstruir los hechos y atribuir responsabilidades.

Por ello, la informática forense y el Derecho trabajan de manera complementaria: la primera aporta las herramientas para descubrir y preservar la evidencia, mientras que el proceso judicial determina su valor y eficacia para acreditar la verdad de los hechos investigados.

ACTIVIDAD 2

Una empresa detecta un ransomware.

En grupos indiquen:

1. ¿Qué medidas adoptarían durante la primera hora?
2. ¿Qué evidencia preservarían?
3. ¿Qué errores evitarían cometer?

BLOQUE V

LA RESPONSABILIDAD DE LOS INTERMEDIARIOS EN INTERNET

Introducción

Internet es una de las mayores herramientas de comunicación creadas por la humanidad.

Millones de personas intercambian información, realizan operaciones comerciales, trabajan, estudian y ejercen su libertad de expresión a través de plataformas digitales.

Sin embargo, detrás de cada búsqueda, publicación o mensaje existen numerosos actores que hacen posible el funcionamiento de la red.

Estos actores son conocidos jurídicamente como **intermediarios digitales**.

Su participación resulta indispensable para el ecosistema de Internet, pero también plantea una de las cuestiones más debatidas del Derecho contemporáneo:

¿Hasta qué punto deben responder por los contenidos que generan sus usuarios?

La respuesta no es sencilla.

Exigirles un control absoluto podría afectar seriamente la libertad de expresión.

Liberarlos completamente de responsabilidad podría dejar sin protección derechos fundamentales como el honor, la intimidad o la privacidad.

El desafío consiste en encontrar un equilibrio razonable entre estos intereses constitucionales.

¿Qué es un intermediario digital?

Un intermediario es una persona o empresa que participa en la circulación, almacenamiento o localización de información generada por terceros, sin ser necesariamente su autor.

No produce el contenido, pero facilita que ese contenido llegue a otros usuarios.

Su intervención puede consistir en brindar acceso a Internet, alojar información, organizarla o ponerla a disposición del público.

Desde la perspectiva jurídica, su papel es particularmente complejo porque ocupa una posición intermedia entre quien publica el contenido y quien resulta afectado por él.

Los distintos tipos de intermediarios

No todos los intermediarios cumplen la misma función.

Por ello, tampoco pueden tener exactamente las mismas obligaciones.

Es importante distinguir sus diferentes roles.

---

1. ISP (Internet Service Provider)

Concepto

El ISP o proveedor de acceso es la empresa que brinda conectividad a Internet.

Su función consiste en permitir que los usuarios puedan conectarse a la red y transmitir datos.

En principio, el ISP no crea, modifica ni controla el contenido que circula por sus redes.

Actúa como un transportista de información.

Podría compararse con una empresa de correo que traslada cartas sin conocer necesariamente su contenido.

Ejemplos

- empresas proveedoras de fibra óptica;
- servicios de Internet por cable;
- operadores de telefonía móvil con acceso a datos;
- proveedores de Internet satelital.

Responsabilidad

En términos generales, el ISP cumple una función técnica de transmisión y no ejerce un control previo sobre la información que circula por su infraestructura.

Por ello, su responsabilidad suele ser excepcional y dependerá de circunstancias particulares previstas por la ley o determinadas por una orden judicial.

---

2. Hosting

Concepto

El servicio de hosting consiste en almacenar información o sitios web en servidores para que puedan ser accesibles desde Internet.

El proveedor pone a disposición el espacio de almacenamiento, pero normalmente no crea los contenidos que allí se alojan.

Ejemplo

Una empresa contrata un servicio para alojar su página institucional.

El proveedor de hosting almacena técnicamente el sitio, pero el contenido fue creado por la empresa cliente.

Importancia jurídica

El hosting posee una capacidad mayor para intervenir sobre el contenido que un ISP.

Puede suspender un sitio, eliminar archivos o restringir el acceso.

Por ello, cuando adquiere conocimiento de la existencia de contenido manifiestamente ilícito, pueden surgir deberes de actuación.

---

3. Buscadores

Concepto

Los buscadores organizan la enorme cantidad de información disponible en Internet mediante procesos automáticos de indexación.

No crean el contenido.

Simplemente localizan páginas existentes y las presentan ordenadas según determinados algoritmos.

Su función es facilitar el acceso a la información.

Ejemplo

Cuando un usuario realiza una búsqueda en Internet, el buscador no genera las noticias ni las imágenes.

Únicamente proporciona enlaces hacia contenidos publicados por terceros.

Particularidad jurídica

El buscador actúa como un intermediario entre el usuario y el sitio de origen.

Su intervención consiste en indexar y vincular información ya existente.

Por ello, uno de los principales debates consiste en determinar cuándo debe eliminar resultados o desindexar contenidos presuntamente ilícitos.

---

4. Plataformas digitales y redes sociales

Concepto

Las plataformas digitales permiten que millones de usuarios publiquen, compartan e intercambien contenidos.

Funcionan como espacios virtuales de interacción social.

A diferencia de un simple proveedor de acceso, participan activamente en la organización y difusión de la información mediante algoritmos de recomendación y sistemas automatizados.

Ejemplos

- redes sociales;
- plataformas de videos;
- servicios de alojamiento de contenido;
- foros;
- aplicaciones colaborativas.

Un rol cada vez más activo

Las plataformas modernas no solo alojan publicaciones.

También las clasifican, recomiendan, viralizan y priorizan mediante algoritmos.

Esta circunstancia ha generado un intenso debate acerca de si continúan siendo meros intermediarios o si desempeñan un papel más activo en la difusión del contenido.

¿Deben controlar todo lo que publican sus usuarios?

Esta es una de las preguntas más importantes del Derecho Digital actual.

A primera vista podría parecer razonable exigir que toda plataforma controle previamente cada contenido antes de su publicación.

Sin embargo, una obligación de ese tipo plantearía enormes dificultades prácticas y constitucionales.

Cada minuto se publican millones de mensajes, fotografías y videos en todo el mundo.

Resulta prácticamente imposible realizar un control humano previo sobre semejante volumen de información.

Además, un sistema de censura preventiva podría afectar gravemente la libertad de expresión.

Por otra parte, si las plataformas nunca respondieran por los contenidos ilícitos difundidos a través de sus servicios, quedarían desprotegidos derechos fundamentales de terceros.

La solución jurídica debe buscar un equilibrio entre ambos intereses.

La tensión entre derechos constitucionales

La responsabilidad de los intermediarios pone en conflicto diversos derechos reconocidos por la Constitución Nacional.

Entre ellos se destacan:

- la libertad de expresión;
- el derecho al honor;
- el derecho a la intimidad;
- la protección de los datos personales;
- el acceso a la información.

Todos estos derechos poseen jerarquía constitucional.

Por ello, ninguno puede imponerse de manera absoluta sobre los demás.

Corresponde armonizarlos caso por caso.

¿Qué ocurriría si existiera un control previo obligatorio?

Si una plataforma estuviera obligada a revisar absolutamente todo antes de permitir su publicación, podrían producirse importantes consecuencias negativas.

Entre ellas:

- demoras incompatibles con la dinámica de Internet;
- eliminación preventiva de contenidos lícitos por temor a responsabilidades;
- limitaciones al debate público;
- afectación de la libertad de expresión;
- incremento de la censura privada mediante algoritmos.

En consecuencia, la mayoría de los sistemas jurídicos rechaza la existencia de un deber general de monitoreo previo.

El criterio adoptado en Argentina

Nuestro país no cuenta con una ley específica que regule integralmente la responsabilidad de los intermediarios digitales.

En consecuencia, el régimen ha sido construido principalmente por la jurisprudencia.

El criterio predominante sostiene que, como regla general, **no existe un deber de controlar preventivamente todos los contenidos publicados por terceros**.

Sin embargo, la situación cambia cuando el intermediario adquiere conocimiento efectivo de una ilicitud concreta y posee la posibilidad razonable de actuar para impedir o limitar el daño.

Los tres elementos centrales

La responsabilidad suele analizarse considerando la concurrencia de tres factores.

1. Conocimiento efectivo

El intermediario debe haber tomado conocimiento de la existencia de un contenido presuntamente ilícito.

Ese conocimiento puede provenir, según el caso, de una orden judicial, una notificación formal o un mecanismo idóneo de denuncia.

No basta una sospecha genérica.

Debe existir una identificación suficientemente precisa del contenido cuestionado.

---

2. Posibilidad de actuar

El intermediario debe contar con medios técnicos y jurídicos para adoptar alguna medida razonable.

No puede exigirse aquello que resulte materialmente imposible.

Por ejemplo, un proveedor de acceso no posee las mismas capacidades que una plataforma que administra directamente el contenido publicado.

---

3. Omisión de actuar

Si, pese a conocer la ilicitud y poder intervenir, el intermediario permanece inactivo, puede surgir responsabilidad por esa omisión.

En este punto, la conducta esperada consiste en adoptar medidas razonables para limitar el daño conforme a las circunstancias del caso.

El caso "Rodríguez c/ Google"

Uno de los precedentes más importantes en esta materia fue el caso "**Rodríguez c/ Google**", resuelto por la Corte Suprema de Justicia de la Nación.

La controversia surgió porque determinados resultados de búsqueda vinculaban el nombre e imagen de una persona con sitios de contenido sexual sin su consentimiento.

La cuestión central consistía en determinar si el buscador debía responder automáticamente por esos contenidos.

El criterio de la Corte Suprema

La Corte sostuvo que los buscadores no son, en principio, autores del contenido generado por terceros.

Su función consiste en indexar información existente mediante procesos automáticos.

Por ello, **no corresponde atribuirles una responsabilidad automática por todo aquello que aparece en los resultados de búsqueda**.

No obstante, cuando adquieren conocimiento efectivo sobre un contenido manifiestamente ilícito y no adoptan medidas razonables dentro de sus posibilidades, puede analizarse la existencia de responsabilidad.

Este precedente continúa siendo uno de los pilares del régimen argentino en materia de intermediarios digitales.

Derecho comparado

Las distintas jurisdicciones del mundo han adoptado soluciones diversas respecto de la responsabilidad de las plataformas.

Estados Unidos

El modelo estadounidense ha privilegiado históricamente una amplia protección para los intermediarios digitales.

La finalidad ha sido fomentar la innovación tecnológica y preservar la libertad de expresión en Internet.

En consecuencia, las plataformas cuentan con un importante margen de inmunidad respecto de contenidos publicados por terceros, salvo determinadas excepciones.

Unión Europea

El modelo europeo presenta un enfoque diferente.

Las grandes plataformas deben cumplir crecientes obligaciones de diligencia, transparencia, evaluación de riesgos y mecanismos eficaces para la gestión de contenidos ilícitos.

Se exige una participación más activa en la prevención y mitigación de daños, especialmente cuando el volumen de usuarios y el impacto social de la plataforma son muy elevados.

Tendencias actuales

La evolución tecnológica ha modificado profundamente el papel de las plataformas digitales.

Los algoritmos ya no solo almacenan información.

También seleccionan, recomiendan y amplifican determinados contenidos.

Por ello, la tendencia internacional apunta hacia un incremento progresivo de las obligaciones de transparencia, moderación responsable y cooperación con las autoridades competentes.

No obstante, continúa existiendo un intenso debate sobre el alcance de esos deberes y sobre el riesgo de afectar la libertad de expresión mediante mecanismos excesivos de control.

Actividad para el aula

Analicen el siguiente caso.

Un usuario publica en una red social una acusación falsa contra una persona, acompañada de una fotografía manipulada digitalmente.

La víctima denuncia el contenido ante la plataforma.

Durante varias semanas no recibe respuesta y la publicación continúa viralizándose.

Respondan:

1. ¿La plataforma es autora del contenido?

2. ¿Qué importancia tiene que haya recibido una notificación formal?
3. ¿Podría existir responsabilidad por la falta de actuación?
4. ¿Qué medidas razonables debería adoptar una plataforma frente a una denuncia de este tipo?

Fundamenten la respuesta considerando la tensión existente entre libertad de expresión, derecho al honor y derecho a la intimidad.

Conclusión

La responsabilidad de los intermediarios constituye uno de los temas más complejos del Derecho Digital contemporáneo.

Internet solo puede funcionar gracias a la participación de múltiples actores técnicos que facilitan el acceso, almacenamiento y difusión de información.

Sin embargo, el enorme poder que poseen las grandes plataformas también implica importantes responsabilidades frente a la protección de los derechos fundamentales.

El modelo argentino, construido principalmente por la jurisprudencia, procura equilibrar esos intereses evitando tanto la censura previa como la impunidad frente a contenidos manifiestamente ilícitos.

Comprender este equilibrio resulta esencial para quienes desarrollarán sistemas informáticos, administrarán plataformas digitales o diseñarán tecnologías que impactarán directamente sobre millones de usuarios.

ACTIVIDAD 3

Diseñen un procedimiento de recepción de denuncias para una red social.

Debe incluir:

- recepción;

- validación;
- preservación de evidencia;
- decisión;
- registro de auditoría;
- posibilidad de apelación.

BLOQUE VI

LEY 25.326 Y CIBERSEGURIDAD

Introducción

En la actualidad, la información constituye uno de los activos más valiosos de cualquier organización.

Empresas, organismos públicos, universidades, bancos, hospitales y plataformas digitales almacenan diariamente enormes cantidades de datos personales de sus usuarios, clientes y empleados.

La protección de esa información no es únicamente una cuestión tecnológica.

También constituye una **obligación jurídica**.

Por ello, el Derecho exige que quienes tratan datos personales adopten medidas adecuadas para impedir accesos no autorizados, pérdidas, alteraciones o divulgaciones indebidas.

La seguridad informática y la protección de datos personales son, hoy, dos disciplinas inseparables.

La Ley 25.326 de Protección de Datos Personales

La Ley 25.326 regula el tratamiento de los datos personales en Argentina.

Su finalidad principal es garantizar el derecho a la privacidad y proteger a las personas frente al uso indebido de su información.

Uno de sus principios fundamentales es el **deber de seguridad**, que obliga a quienes administran bases de datos a implementar medidas técnicas y organizativas destinadas a preservar la información.

No basta con obtener legalmente los datos.

También es necesario protegerlos durante todo su ciclo de vida.

El deber de seguridad

Toda organización que trata datos personales debe adoptar medidas razonables para evitar:

- la pérdida de información;
- la destrucción de datos;
- la alteración no autorizada;
- el acceso ilegítimo;
- la divulgación indebida;
- el tratamiento no autorizado.

Este deber alcanza tanto a organismos públicos como privados.

La intensidad de las medidas dependerá del tipo de información tratada y del riesgo existente.

No es lo mismo proteger una lista pública de clientes que una base de datos con historias clínicas o información financiera.

La seguridad como obligación jurídica

Con frecuencia se considera que la ciberseguridad es un problema exclusivamente técnico.

Sin embargo, desde el punto de vista jurídico constituye una obligación legal.

Una empresa que no implementa medidas razonables puede incurrir en responsabilidad administrativa, civil e incluso penal, dependiendo de las consecuencias del incidente.

Por ello, las decisiones tecnológicas poseen un impacto directo sobre el cumplimiento normativo.

¿Qué medidas de seguridad se consideran adecuadas en la actualidad?

La evolución constante de las amenazas obliga a actualizar permanentemente las políticas de seguridad.

Entre las medidas más relevantes pueden mencionarse las siguientes.

---

1. Autenticación multifactor (MFA)

La autenticación multifactor exige que el usuario acredite su identidad mediante más de un mecanismo.

Por ejemplo:

- contraseña;
- código enviado al teléfono móvil;
- aplicación autenticadora;
- llave criptográfica;
- dato biométrico.

Esta medida reduce significativamente el riesgo derivado del robo de credenciales.

En la actualidad constituye una de las herramientas más eficaces para prevenir accesos ilegítimos.

---

2. Gestión de privilegios

No todos los usuarios necesitan acceder a toda la información.

El principio de **mínimo privilegio** establece que cada persona debe contar únicamente con los permisos estrictamente necesarios para cumplir sus funciones.

Una correcta administración de permisos disminuye el riesgo de accesos indebidos y limita el impacto de un eventual incidente.

En programación, este principio suele implementarse mediante sistemas de roles y permisos (RBAC).

---

3. Backups o copias de seguridad

Las copias de respaldo permiten recuperar la información frente a incidentes como:

- fallas técnicas;
- errores humanos;
- ataques de ransomware;
- sabotajes internos;
- desastres naturales.

Sin embargo, realizar backups no es suficiente.

También deben probarse periódicamente los procedimientos de restauración para verificar que puedan recuperarse correctamente.

Un backup que nunca fue probado puede resultar inútil en una situación crítica.

4. Monitoreo continuo

El monitoreo permite detectar comportamientos anómalos antes de que produzcan daños mayores.

Mediante herramientas especializadas pueden identificarse:

- intentos reiterados de acceso;
- conexiones desde ubicaciones inusuales;
- movimientos laterales dentro de la red;
- elevaciones de privilegios;
- transferencias masivas de información.

Una detección temprana reduce considerablemente el impacto de un incidente de seguridad.

---

5. Registros de auditoría (logs)

Los logs constituyen una de las principales fuentes de evidencia digital.

Permiten reconstruir qué ocurrió, cuándo ocurrió y quién realizó cada acción.

Un adecuado sistema de auditoría registra, entre otros aspectos:

- inicios de sesión;
- modificaciones de datos;
- creación de usuarios;
- cambios de permisos;
- operaciones críticas;
- intentos fallidos de autenticación.

Desde la perspectiva jurídica, los registros de auditoría poseen enorme importancia probatoria.

Muchas investigaciones informáticas dependen casi exclusivamente de ellos.

6. Capacitación del personal

La tecnología por sí sola no elimina el riesgo.

Gran parte de los incidentes de seguridad se originan por errores humanos.

Entre los ejemplos más frecuentes se encuentran:

- apertura de archivos maliciosos;
- clic en enlaces fraudulentos;
- utilización de contraseñas débiles;
- reutilización de credenciales;
- divulgación involuntaria de información.

Por ello, la capacitación periódica del personal constituye una medida esencial de prevención.

La seguridad informática también depende del comportamiento de las personas.

La relación entre ciberseguridad y prueba judicial

Una política adecuada de seguridad no solo protege los activos de una organización.

También facilita enormemente la producción de prueba en un proceso judicial.

Cuando ocurre un incidente, la existencia de registros completos, sistemas de auditoría y procedimientos documentados permite reconstruir los hechos con mayor precisión.

Por el contrario, una infraestructura sin registros o con controles deficientes dificulta la investigación y puede impedir determinar responsabilidades.

Seguridad preventiva y responsabilidad jurídica

Implementar medidas preventivas reduce la probabilidad de sufrir incidentes y, además, demuestra que la organización actuó con la diligencia exigible.

En caso de un ataque informático, la existencia de políticas de seguridad adecuadas puede constituir un elemento relevante para evaluar la responsabilidad de la empresa.

La ausencia de controles básicos puede interpretarse como una conducta negligente.

Caso práctico para analizar en clase

Una empresa almacena los datos personales de miles de clientes.

Todos los empleados utilizan la misma contraseña para acceder al sistema.

No existen registros de auditoría ni copias de seguridad.

Un atacante obtiene las credenciales mediante phishing, elimina la base de datos y publica información confidencial.

Preguntas para debatir:

1. ¿Qué medidas de seguridad omitió implementar la empresa?
2. ¿Qué dificultades probatorias aparecerán durante la investigación?
3. ¿Podría existir responsabilidad civil por la falta de medidas adecuadas?
4. ¿Qué cambios propondrían desde una perspectiva técnica y jurídica?

Conclusión

La protección de los datos personales constituye una obligación legal y una necesidad estratégica para cualquier organización.

Las medidas de ciberseguridad no solo previenen incidentes, sino que también generan evidencia confiable para reconstruir los hechos cuando ocurre un ataque.

En el Derecho Digital moderno, seguridad informática y cumplimiento normativo forman parte de una misma política integral de gestión de riesgos.

BLOQUE VII

EL CONVENIO DE BUDAPEST Y LA COOPERACIÓN INTERNACIONAL EN CIBERDELITOS

Introducción

Internet ha eliminado las fronteras físicas para la circulación de la información.

Sin embargo, los sistemas jurídicos continúan organizados territorialmente.

Esta diferencia genera enormes dificultades para investigar delitos informáticos.

Un atacante puede encontrarse en un país, utilizar servidores ubicados en otro y afectar víctimas localizadas en un tercero.

En ese contexto, la cooperación internacional resulta indispensable.

El principal instrumento jurídico destinado a facilitar esa cooperación es el **Convenio de Budapest sobre Ciberdelincuencia**.

¿Qué es el Convenio de Budapest?

Es un tratado internacional elaborado por el Consejo de Europa con el objetivo de armonizar la legislación penal sobre ciberdelitos y facilitar la cooperación entre los Estados.

Constituye el instrumento internacional más importante en materia de investigación y persecución de delitos informáticos.

Argentina adhirió al Convenio mediante la **Ley 27.771**, incorporándose al sistema internacional de cooperación en esta materia.

¿Por qué es necesario un tratado internacional?

Los ciberdelitos presentan características que dificultan enormemente su investigación.

Por ejemplo:

- el autor puede actuar desde otro continente;
- los servidores pueden estar distribuidos en varios países;
- las pruebas pueden almacenarse en servicios internacionales;
- los registros pueden eliminarse en pocos minutos.

Sin mecanismos rápidos de cooperación, gran parte de la evidencia desaparecería antes de que pudiera obtenerse legalmente.

Los objetivos del Convenio

El Convenio busca fortalecer la lucha contra la ciberdelincuencia mediante la coordinación entre los Estados.

Sus principales objetivos son:

- armonizar las legislaciones nacionales;

- facilitar investigaciones internacionales;
- acelerar la obtención de evidencia digital;
- mejorar la cooperación judicial y policial;
- promover estándares comunes en materia de ciberdelitos.

Preservación rápida de la evidencia digital

Uno de los aportes más importantes del Convenio consiste en permitir la preservación urgente de evidencia electrónica.

La información digital puede modificarse o eliminarse en cuestión de segundos.

Por ello, resulta fundamental solicitar rápidamente su conservación antes de iniciar procedimientos más complejos de obtención.

Esta preservación evita que datos esenciales para una investigación desaparezcan.

Intercambio internacional de información

Las investigaciones sobre ciberdelitos requieren con frecuencia obtener información ubicada fuera del país.

El Convenio establece mecanismos para facilitar el intercambio de datos entre las autoridades competentes de distintos Estados.

Ello permite acceder con mayor rapidez a registros, direcciones IP, información de proveedores de servicios y otros elementos relevantes para la investigación.

Asistencia judicial internacional

Los Estados parte se comprometen a colaborar mutuamente mediante mecanismos de asistencia jurídica.

Esta cooperación puede incluir:

- obtención de pruebas digitales;
- ejecución de medidas de investigación;
- intercambio de documentación;
- identificación de responsables;
- preservación de información almacenada en servidores extranjeros.

La finalidad es evitar que las fronteras nacionales se conviertan en un obstáculo para la persecución penal.

Cooperación entre organismos especializados

El Convenio también promueve la creación de puntos de contacto permanentes para atender solicitudes urgentes de cooperación.

Estos mecanismos permiten que las autoridades intercambien información de manera rápida cuando el tiempo resulta determinante para preservar la evidencia.

En materia informática, una demora de pocas horas puede implicar la pérdida definitiva de registros esenciales.

Un ejemplo práctico

Imaginemos el siguiente supuesto:

Un ciudadano argentino sufre una estafa mediante una plataforma digital.

El atacante opera desde otro país, utiliza un servidor ubicado en un tercero y recibe el dinero en una cuenta radicada en una cuarta jurisdicción.

Sin mecanismos internacionales de cooperación, la investigación quedaría prácticamente paralizada.

Gracias al Convenio de Budapest, los Estados pueden coordinar acciones para preservar evidencia, intercambiar información y asistir a las autoridades encargadas de la investigación.

La importancia para los futuros programadores

Aunque muchos desarrolladores no participarán directamente en investigaciones penales, sí diseñarán sistemas que almacenan información potencialmente relevante para la Justicia.

Por ello, resulta fundamental comprender la importancia de:

- conservar registros de auditoría;
- implementar políticas de retención de datos;
- preservar la integridad de los logs;
- documentar incidentes de seguridad;
- colaborar con requerimientos judiciales conforme al marco legal vigente.

Una arquitectura correctamente diseñada puede facilitar significativamente la reconstrucción de un hecho investigado.

Actividad para el aula

Analicen el siguiente caso:

Una empresa argentina sufre un ataque de ransomware.

La investigación determina que el malware fue distribuido desde un servidor ubicado en Europa y que el dinero del rescate fue transferido a una billetera virtual administrada desde otro continente.

Respondan:

1. ¿Qué dificultades presenta una investigación de estas características?
2. ¿Por qué resulta necesaria la cooperación internacional?
3. ¿Qué tipo de evidencia debería preservarse inmediatamente?
4. ¿Cómo contribuye el Convenio de Budapest a la investigación?

Conclusión

La ciberdelincuencia constituye un fenómeno global que trasciende las fronteras nacionales.

Por ello, ningún Estado puede enfrentarla de manera aislada.

El Convenio de Budapest representa el principal marco internacional de cooperación para la investigación de delitos informáticos, facilitando la preservación de evidencia, el intercambio de información y la asistencia judicial entre países.

En un mundo digital e interconectado, la cooperación internacional se convierte en una herramienta tan importante como la propia tecnología para garantizar la eficacia del Derecho Penal.

CASO INTEGRADOR FINAL

Un ex empleado conserva sus credenciales luego de ser desvinculado.

Ingresa al sistema de la empresa.

Descarga la base de clientes.

Publica parte de la información en Internet.

Exige dinero para eliminarla.

Analicen:

1. ¿Qué delitos podrían configurarse?

2. ¿Qué evidencia digital preservarían?
3. ¿Qué responsabilidad podría tener la empresa respecto de sus clientes?
4. ¿Qué medidas de seguridad habrían evitado el incidente?
5. ¿Qué cooperación internacional sería necesaria si el servidor estuviera ubicado en otro país?

CIERRE

Tres ideas para recordar:

1. Los delitos informáticos protegen bienes jurídicos específicos como la confidencialidad, la integridad, la disponibilidad, el patrimonio y la privacidad.
2. La evidencia digital solo resulta útil si es preservada correctamente mediante una adecuada cadena de custodia.
3. En el ecosistema digital, la tecnología y el derecho son disciplinas complementarias: una buena arquitectura de seguridad puede prevenir un incidente y, al mismo tiempo, proporcionar la evidencia necesaria para acreditar un delito ante los tribunales.
