USERS

Técnico en
REDES &SEGURIDAD

3

ASPECTOS LEGALES

CONOZCA LAS RESPONSABILIDADES DE UN ADMINISTRADOR DE REDES EN EL ÁMBITO LEGAL

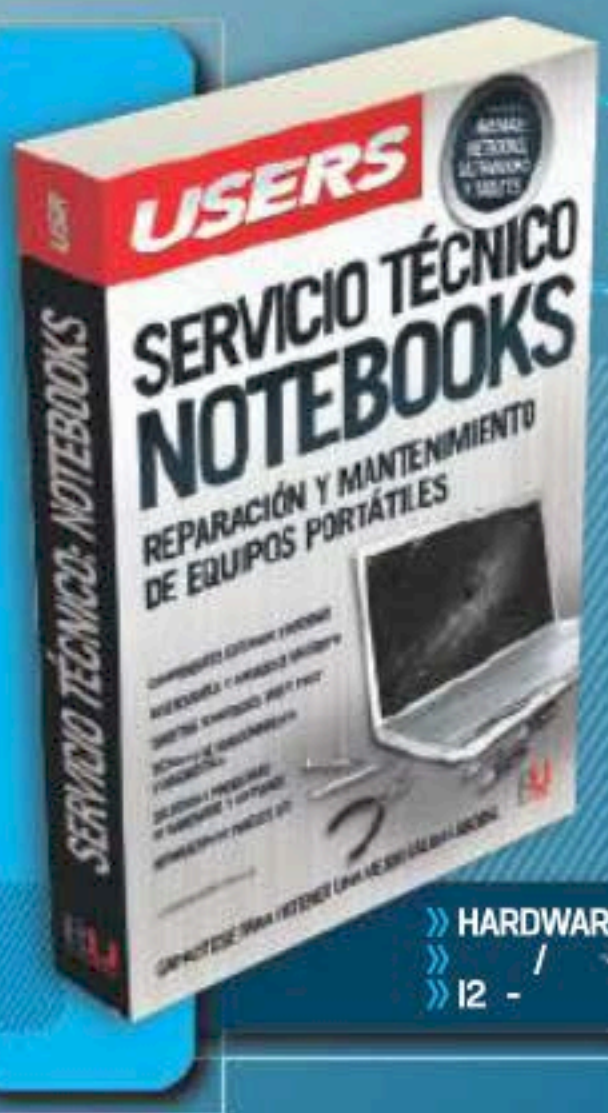
- DELITOS INFORMÁTICOS
- DATOS PERSONALES Y PRIVACIDAD
- CONTROL EN EL AMBITO LABORAL
- LEYES Y JURISPRUDENCIA

Autor: Darío Veltani

CONÉCTESE
CON LOS MEJORES LIBROS DE COMPUTACIÓN

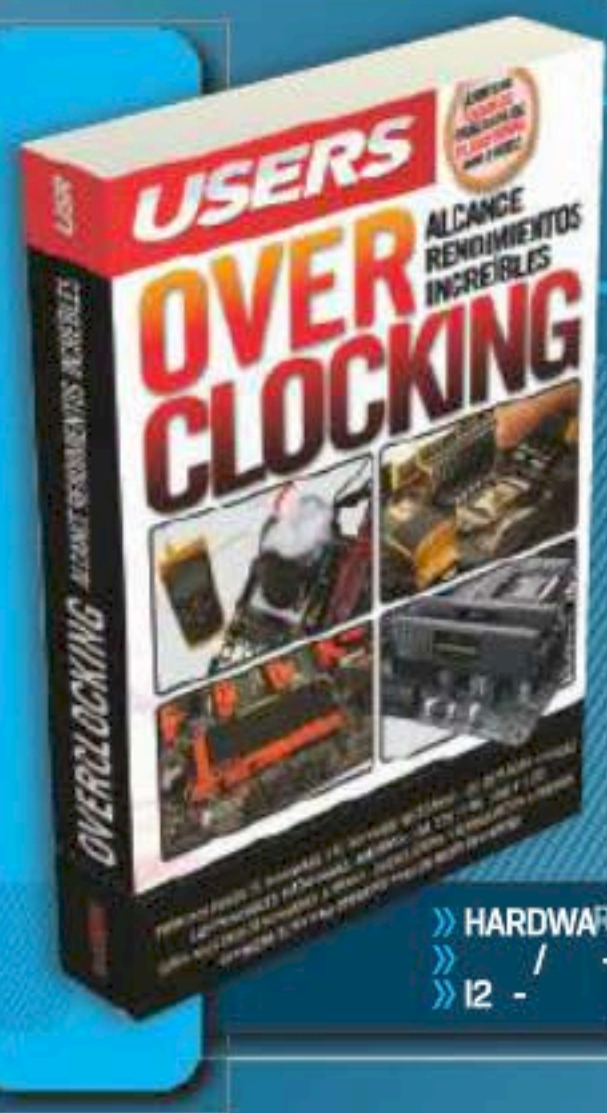
LLEGAMOS A TODO EL MUNDO
VÍA OCA * Y DHL **
usershop.redusers.com
usershop@redusers.com
+54 (011) 4110-8700

* SÓLO VÁLIDO EN LA REPÚBLICA ARGENTINA. ** VÁLIDO EN TODO EL MUNDO EXCEPTO ARGENTINA



CAPACÍTESE PARA OBTENER UNA MEJOR SALIDA LABORAL

» HARDWARE / MOBILE
» / - 2
» I2 -

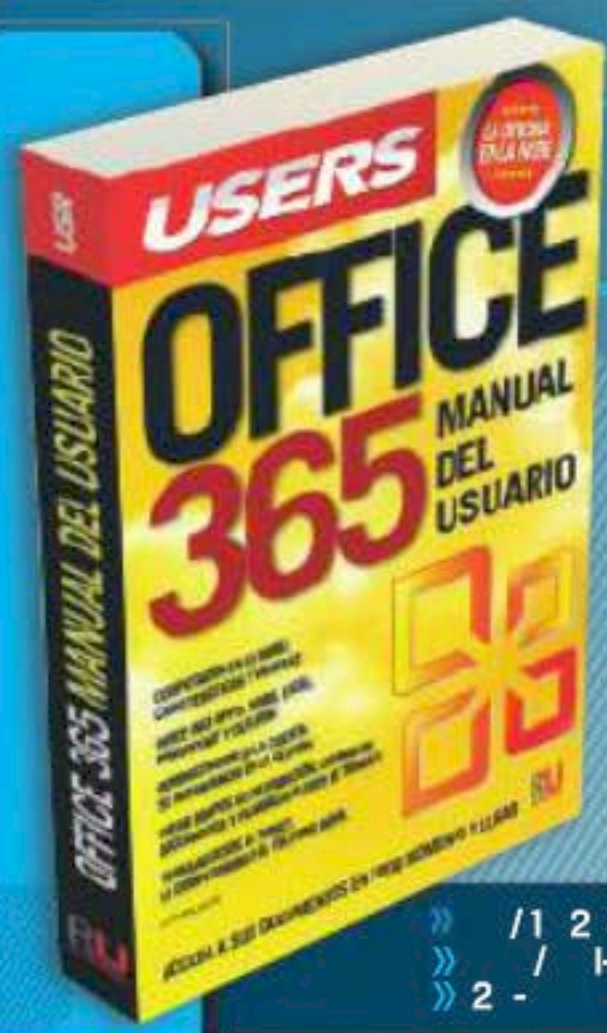


ALCANCE RENDIMIENTOS INCREÍBLES EN SU PC

» HARDWARE
» / - 2
» I2 -

APRENDA A PROGRAMAR SIN CONOCIMIENTOS PREVIOS

» DE ARROL .
» / I- 2
» 2 -



ACCEDA A SUS DOCUMENTOS EN TODO MOMENTO Y LUGAR.

» /1 2 2 -31- 3
» / I- 2
» 2 -

USERS

Técnico en REDES &SEGURIDAD

TÍTULO: Aspectos legales
AUTOR: Juan Darío Veltani
COLECCIÓN: Pocket Users
FORMATO: 13.5 x 19 cm
PÁGINAS: 96

Primera impresión realizada en enero de MMXIII.

Sevagraf, Costa Rica 5226, Grand Bourg, Malvinas Argentinas, Pcia. De Buenos Aires.

ISBN 978-987-1857-77-7

Veltani, Juan Darío
Aspectos legales. - 1a ed. - Buenos Aires: Fox Andina, 2013.
96 p.; 19 x14 cm. - (Pocket users; 28)
ISBN 978-987-1857-77-7

1. Informática. I. Título
CDD 004

El **autor**

Darío Veltani

Es abogado y docente universitario. Dicta clases en programas vinculados con la tecnología en general, como la Maestría en Explotación de Datos y Gestión del Conocimiento (Universidad Austral). Es coordinador académico de la carrera de Especialización en Derecho de la Alta Tecnología (Universidad Católica Argentina), profesor en la Diplomatura en Propiedad Intelectual (Argentina-Paraguay) y en la Maestría en Propiedad Intelectual (Universidad Austral). Asesora empresas en asuntos vinculados principalmente con el Derecho y la Tecnología.

Prólogo **al contenido**

A primera vista, el Derecho y la Informática parecen dos paralelas. En efecto, para quienes no están habituados a su estudio, el Derecho aparece como una disciplina estática, tradicional y conservadora, y la Informática, como una actividad en constante movimiento.

Sin embargo, todas las actividades humanas se encuentran reguladas por el Derecho. Por lo tanto, resulta conveniente que quienes ejercen su profesión en el ámbito informático conozcan los principios jurídicos básicos con los que se juzgará su actuación.

La finalidad de esta obra es que los lectores comprendan cómo se relacionan los preceptos legales con su actividad. En este sentido, debemos aclarar que los conceptos que se desarrollarán, en muchos casos, han sido simplificados para facilitar su comprensión.

En definitiva, la lectura de esta obra permitirá a los administradores de redes identificar aquellas actividades que podrían exponerlos en términos personales y hasta implicar la comisión de un delito. De este modo, tendrán herramientas para tomar las decisiones que, en cada caso, resulten más adecuadas.

Contenido **del libro**

Capítulo 1

Las tecnologías de la información y el Derecho

Veremos cómo aplicar las leyes pensadas para un mundo físico a las tecnologías de la información.

RedUSERS.com

Introducción

En los últimos años, las **tecnologías de la información** (IT) generaron importantes cambios culturales en la sociedad. Tal vez quienes trabajan a diario con ellas no sean conscientes de la importancia de estas transformaciones, que afectan aspectos de la vida no solo personal y familiar, sino también profesional y laboral y, en general, el modo en que concebimos las relaciones sociales.

Figura 1. **Las tecnologías de la información han cambiado el modo en que concebimos el trabajo y nuestras relaciones.**

Algunos aspectos positivos de los avances tecnológicos están vinculados al hecho de que, en términos generales, han permitido optimizar y hacer más eficiente el trabajo, como así también, acortar las distancias físicas entre las personas.

Ahora bien, junto con estas ventajas, comenzaron a aparecer algunos problemas derivados del uso de las tecnologías de la información. Es que, entre otras cosas, la gran capacidad de procesamiento de información permitió desarrollar sistemas de vigilancia que podrían atentar contra la privacidad de las personas. También empezaron a aparecer nuevos **daños**, que antes hubieran sido impensados (por ejemplo, la difamación o afectación de la reputación online).

En el ámbito del derecho penal, se potenció la comisión de ciertos delitos relacionados con

NUEVOS DAÑOS INFORMÁTICOS
Difamación en redes sociales o blogs por parte de los denominados trolls, que se dedican a agraviar a otros amparándose en perfiles falsos o anónimos.
Aprovechamiento de la estructura de Internet para copiar y distribuir de manera ilegítima libros, películas, software y todo tipo de obras.
Registro de un sitio de Internet a fin de obtener una compensación económica del titular de la marca y/o de quien tenga los derechos legítimos para registrarlo (cybersquatting).
Alteración del software con el fin de eludir medidas de seguridad que impidan su copia o distribución (comúnmente denominadas DRMs).

Tabla 1. **Día a día surgen nuevos delitos informáticos.**

Figura 2. **Las IT permitieron desarrollar sistemas de vigilancia electrónica, que pueden resultar violatorios de la privacidad.**

la violación de derechos de propiedad intelectual. Y también surgieron **nuevos delitos**, que debieron ser regulados específicamente, como, por ejemplo, lo atinente al hacking, el daño informático, la defraudación informática, el cyberbulling, etcétera.

APLICACIÓN DE NORMAS DEL MUNDO FÍSICO AL MUNDO VIRTUAL

Todas estas situaciones determinaron un verdadero desafío para el Derecho, ya que no existían normas que las contemplaran específicamente. En efecto, debemos recordar que el Derecho es la ciencia que tiene como finalidad regular la vida en sociedad, de un modo que resulte razonable y, además, previsible.

Las leyes no pueden ser modificadas constantemente, porque esto generaría **inseguridad jurídica**, ya que nadie sabría qué está bien y qué está mal. Algo similar ocurre con los criterios judiciales, que no pueden variar de un modo sustancial en muy poco tiempo.

Las **leyes tradicionales** fueron concebidas para un mundo en el que las **cosas** eran tangibles; todo se veía y se podía **tocar**. Y los razonamientos en que se fundaron esas leyes y su

TECNOLOGÍAS DE LA INFORMACIÓN

El Diccionario Merriam Webster On Line las define como las tecnologías vinculadas al desarrollo, mantenimiento y uso de sistemas informáticos, software y redes informáticas para el procesamiento y la distribución de datos (www.merriam-webster.com).

Figura 3.
En el hacking, el delincuente accede y, eventualmente, toma el control de una computadora.

interpretación por parte de los jueces también tenían la misma lógica. Como ejemplo, podemos mencionar el **hurto**, un delito que implica el desapoderamiento de una cosa, es decir, **sacarle esa cosa** a alguien (como podría ser el caso de una persona que, sin violencia, le quita la cartera a otra). En casi todas las legislaciones latinoamericanas, el hurto se encuentra legislado. Ahora bien, ¿podríamos decir que hay hurto cuando lo que ocurre es que alguien **copia** cierta información, pero deja el archivo original en el mismo lugar en que estaba? En este caso, la información –entendida como el archivo que se copió– nunca sale del ámbito de custodia de su titular, a diferencia de lo que ocurre con el ejemplo de la cartera.

Entonces, cuando estos casos aparecen y los jueces deben interpretar las normas tradicionales para aplicarlas a casos vinculados a tecnologías de la información, las respuestas no siempre son adecuadas.

EL COMMON LAW

Es uno de los sistemas jurídicos del mundo occidental. Tiene su origen en Inglaterra en la Edad Media y se funda en la interpretación que hacen los jueces ante situaciones conflictivas, lo que genera precedentes que, luego, son aplicados a casos similares.

Los criterios judiciales no pueden modificarse constantemente

UN PROBLEMA GLOBAL

Esta problemática se da a nivel mundial, aunque presenta mayores inconvenientes en los países latinoamericanos, cuya tradición jurídica es la **continental europea**, dado que en ellos los sistemas jurídicos se encuentran **codificados**, y esto implica que la ley debe estar siempre escrita. Esto no es así en aquellos países con sistemas jurídicos que siguen el denominado **Common Law** (por ejemplo, Estados Unidos), en los cuales no hay muchas leyes, sino que adquiere mayor relevancia la interpretación de los tribunales.

En la actualidad, se ha avanzado mucho en algunos temas de tecnología y derecho –como la regulación de la privacidad y la protección de los datos personales–, para los que existen leyes específicas en casi todo el mundo. Sin embargo, en otras áreas, como los delitos informáticos o la regulación de los medios informáticos

Figura 4. **Resulta complejo aplicar los conceptos tradicionales en materia criminal a los delitos informáticos.**

en el ámbito laboral, el avance no ha sido tan homogéneo y existen importantes diferencias entre las distintas legislaciones.

En este libro nos referiremos a todos estos problemas, procurando brindar una visión predominantemente práctica, que pueda ser de utilidad para los administradores de redes. Ellos, como veremos, están expuestos a diario a situaciones que podrían derivar en potenciales conflictos legales.

CÓDIGO CIVIL

Es otro de los sistemas jurídicos de Occidente. Tiene su origen en Roma, y se basa en que todas las normas deben estar escritas, codificadas; la tarea de los jueces es interpretar dichas normas en situaciones puntuales. Es el sistema adoptado en Latinoamérica.

¿Por qué un administrador de redes **debe leer este libro?**

Las tecnologías de la información, como dijimos, generaron un importante cambio sociocultural en los últimos años. Este cambio estuvo relacionado, en gran medida, con la interconexión de las computadoras y otros dispositivos, para constituir redes informáticas que permitieron ampliar las capacidades de procesamiento.

En este sentido, sin dudas, el ejemplo más claro de la importancia de las redes informáticas es **Internet**, la Red de Redes, pero no es el único. Las redes informáticas están presentes prácticamente en todos lados. Tanto el Estado, como las empresas y cualquier particular que necesite una capacidad de procesamiento o prestaciones mayores de las que puede darle una computadora stand alone debe constituir una red.

Y en este contexto, el **administrador de una red** aparece como una figura de gran relevancia. Es el administrador quien tiene la potestad de fijar los parámetros de seguridad de la red, de asignar perfiles a los distintos usuarios que la utilizan, de monitorear su uso, de establecer normas y hacerlas cumplir, etcétera.

En otras palabras, el funcionamiento de una red está muy vinculado a la figura de su administrador, y esta situación tiene una gran cantidad de consecuencias jurídicas que él debe conocer. Sobre todo, porque parte de ellas implican que el administrador puede ser considerado responsable, en términos personales, de ciertas actividades que se realicen en la red.

Lo que ocurre es que, en relación con el administrador de la red, nos encontramos en la situación que mencionábamos en la introducción del libro, en el sentido de que aún no se han dictado normas que regulen de un modo claro su responsabilidad. Por lo tanto, deben aplicarse las normas tradicionales, que no fueron pensadas para esta actividad.

La falta de normas expresas que se refieran al administrador de la red determina que su cuidado

AVISO LEGAL

Esta obra no pretende agotar el análisis de las cuestiones legales que debe tener en cuenta el administrador de una red, ni brindar un consejo jurídico para un caso en particular. Se trata de dar una orientación sobre lineamientos generales de actuación.

FUNCIONES DEL ADMINISTRADOR DE UNA RED	
Seguridad de la red	El administrador debe establecer parámetros razonables de seguridad para la red. Si bien podría existir una persona distinta de él que tuviera la responsabilidad específica de la seguridad, el administrador siempre tendrá algún grado de responsabilidad en la configuración de la seguridad.
Perfiles de usuario y políticas de uso aceptables	En general, será el administrador de la red quien determine los perfiles de los usuarios y, asimismo, las políticas aceptables de uso. Con relación a este último punto, el administrador también será el responsable de velar por su efectivo cumplimiento.

Tabla 2. **El administrador es una figura imprescindible para evaluar cualquier conducta que ocurra en la red.**

deba ser mayor, porque sus obligaciones legales no están comprendidas en una única ley, sino que provienen de todo el sistema normativo.

Es por eso que en esta obra intentaremos repasar, de un modo sucinto, los distintos ámbitos de responsabilidad del administrador de la red, para que pueda seguir ciertos criterios legales básicos en el desarrollo de sus tareas.

LOS ÁMBITOS DE RESPONSABILIDAD DEL ADMINISTRADOR DE REDES

El administrador de una red debe ajustar su conducta teniendo en cuenta los distintos ámbitos en que esta será evaluada, entre los que podemos distinguir:

- El ámbito civil
- El ámbito penal
- El ámbito laboral
- El ámbito administrativo o regulatorio
- El ámbito profesional

A continuación, nos referiremos brevemente a cada uno de estos ámbitos, pero en este libro trataremos solo los tres primeros y algunos aspectos del cuarto, dado que el ámbito profesional difiere mucho en cada legislación y aún no se ha desarrollado lo suficiente como para poder escribir una obra en términos generales al respecto.

El ámbito civil

Cuando nos referimos al **ámbito civil**, que será tratado en el Capítulo 5, estamos haciendo referencia a la responsabilidad civil del administrador de la red por daños causados a terceros. Es decir, en este ámbito se analizará si corresponde que el administrador responda, en

términos personales, por los daños que pudieran sufrir terceros como consecuencia de las actividades desarrolladas a través de la red. Es importante destacar que, dentro del concepto de **terceros**, también se incluye a los propios usuarios de la red, respecto de quienes el administrador tiene importantes obligaciones de garantía y seguridad.

La casuística en el ámbito de la responsabilidad civil es muy amplia, porque comprende desde el daño padecido por quien vio comprometida cierta información confidencial en virtud de una política de seguridad inadecuada, hasta el daño de quien ha visto perjudicados sus derechos de propiedad intelectual sobre alguna obra que ha sido distribuida ilícitamente a través de la red en virtud de la falta de controles del administrador.

El ámbito penal

En el ámbito de la **responsabilidad penal**, el análisis es completamente diferente del anterior. En este caso, lo que analizaremos es si la conducta del administrador de la red podría estar comprendida dentro de lo que se denomina **delito penal**. Un delito penal es una conducta expresamente identificada como tal en la legislación, y que ha sido considerada tan nociva

Figura 5. **Los delitos penales suelen castigarse con la privación de la libertad.**

para la sociedad, que quien la comete no solo debe indemnizar a la víctima por los daños que hubiera causado, sino que, también, se encuentra sujeto al cumplimiento de una **pena**; esta suele consistir en la privación de la libertad (prisión o reclusión).

Este ámbito será analizado con detenimiento en el Capítulo 3 de esta obra, pero podemos adelantar que los delitos penales –a diferencia de lo que ocurre en el ámbito civil– por lo general implican que la acción debe ser cometida personalmente por el administrador de la red (en estos casos, en principio, este no debería

TERRITORIALIDAD DE LOS DELITOS PENALES

Si bien los delitos penales varían entre los diferentes países, los principios generales aplicables a la responsabilidad penal son similares entre las diversas legislaciones. Por lo tanto, en este ámbito haremos referencia a estándares genéricos de conducta.

Figura 6. El administrador empleado debe cumplir con su trabajo, pero con conciencia de su responsabilidad individual.

responder por acciones delictivas que pudieran cometer los usuarios).

El ámbito laboral

En cuanto al ámbito de la **responsabilidad laboral**, nos referimos a la eventual responsabilidad del administrador de la red en su condición de **empleado** de una organización. En este caso, su conducta deberá ser evaluada dentro del marco de una relación laboral, en la que las decisiones generales sobre la red tal vez serán definidas por la organización, y no, por el propio administrador. Un primer acercamiento a la situación del administrador empleado parece indicar que resulta la más **cómoda**, dado que, al acatar órdenes de la organización, existen ciertos niveles de responsabilidad que no se le aplicarían (por ejemplo, la responsabilidad civil por daños, dado que la responsable será la organización, y no, el administrador, que es empleado y sigue instrucciones). Sin embargo, la condición de empleado, en muchas oportunidades, coloca al administrador en situaciones más complejas que las que enfrenta quien administra una red en forma independiente. Es que si el administrador empleado comete un delito siguiendo órdenes de la organización –por ejemplo, en lo que se refiere al monitoreo de

DERECHO PENAL

Forma parte del Derecho Público, ya que existe un especial interés del Estado en este ámbito. Procura el castigo de las conductas que la sociedad considera más graves en cuanto al daño que generan, y que se denominan delitos penales.

los usuarios–, no podrá ampararse en su condición para eximirse de su responsabilidad penal. Por otro lado, responde ante la organización en caso de que se genere algún daño y terceras personas la demanden por alguna acción del administrador de la red.

Es por eso que, en el Capítulo 4 de esta obra, nos referiremos específicamente al uso de medios informáticos en el ámbito laboral, para que el administrador conozca de un modo general los límites que deberá tener en cuenta en su actuación con el objetivo de no incumplir con sus deberes como empleado de la organización pero, a la vez, de no realizar actos que luego puedan generarle responsabilidad.

El ámbito administrativo o regulatorio

Respecto del **ámbito administrativo o regulatorio**, debemos señalar que, muchas veces, el administrador de la red tiene que tomar contacto con autoridades administrativas, asumiendo responsabilidades por el cumplimiento de diversas normas que exceden sus funciones habituales. Con relación a este tema, la casuística es muy rica y no podríamos abarcarla en este libro, pero nos referiremos a un ámbito administrativo que se encuentra muy desarrollado a nivel normativo, y en el que, habitualmente, se ven involucrados los administradores de redes: el marco regulatorio de la **protección de los datos personales.**

En este sentido, tal como anticipamos en la introducción, tal vez sea este el tema que más desarrollo legislativo ha tenido. Prácticamente todos los países de Europa y gran parte de los países de América Latina poseen legislación específica que protege los datos personales. En estas legislaciones suele estar presente la obligación de declarar y/o registrar las bases de datos que contienen ese tipo de datos personales. El registro, habitualmente, se encomienda a los administradores de la red, quienes luego aparecen en los documentos presentados ante las autoridades administrativas como los **responsables** del cumplimiento de la normativa de protección de datos personales.

Esta responsabilidad del administrador de la red es muy importante, porque lo coloca en relación directa con autoridades administrativas que están llamadas a controlar a la organización para la que él trabaja. Por lo tanto, resulta una responsabilidad claramente exorbitante respecto de la que el administrador de la red

CÓDIGO DE ÉTICA PROFESIONAL

Un código de ética profesional es un conjunto de normas dictadas por la entidad que regula la matrícula, que contiene obligaciones morales y éticas para el ejercicio de la profesión. Su incumplimiento puede generar sanciones para el profesional matriculado.

Figura 7. **En el sitio del COPITEC se puede acceder a su código de ética profesional.**

debería asumir. No obstante, dado que en la práctica se lo designa como responsable frente a las autoridades administrativas, al menos en lo que respecta al régimen de protección de datos personales, en el Capítulo 2 de esta obra nos referiremos a las obligaciones que surgen habitualmente de dicho régimen.

El ámbito profesional

Por último, queda mencionar el **ámbito profesional**. En este sentido, como frecuentemente los administradores de redes poseen títulos profesionales (por ejemplo, ingeniero en Sistemas o ingeniero en Redes), en algunos lugares se requiere de una matrícula habilitante para el ejercicio de dichas actividades. Esto implica que la entidad que tenga la administración de la matrícula (en algunos casos puede ser el Estado en forma directa, y en otro casos puede haberse concedido esta facultad a terceros, como asociaciones profesionales) tendrá también la facultad de ejercer el control disciplinario. Por lo general, para ejercer dicho control, la entidad que administra la matrícula establece **códigos de ética** que deben ser cumplidos por los matriculados, y cuyo incumplimiento trae aparejadas sanciones que pueden llegar hasta la exclusión de la matrícula.

Estas sanciones suelen ser independientes de las eventuales sanciones civiles, administrativas, laborales y penales, por lo que deben ser

DERECHO CIVIL

Se ocupa de las relaciones entre particulares en el ámbito del Derecho Privado (donde no hay un interés específico del Estado). En este ámbito, quien daña a otro debe reparar. El daño puede ocurrir por un hecho ilícito o por el incumplimiento de una obligación.

analizadas en forma específica. No obstante, como en la actualidad no hay uniformidad en cuanto a las exigencias profesionales para los administradores de redes y, además, la colegiación en profesiones vinculadas a los sistemas informáticos no ha tenido aún el desarrollo que puede verse en otras profesiones (por ejemplo, la abogacía), no nos abocaremos específicamente a este tipo de responsabilidad en la presente obra.

RESPONSABILIDAD DEL ADMINISTRADOR DE UNA RED	
Ámbito civil	Se analiza si el administrador debe resarcir los daños ocasionados por el uso de la red y/o por las actividades de los usuarios.
Ámbito penal	Se analiza si la actividad desarrollada por el administrador de la red podría considerarse un delito penal.
Ámbito laboral	El administrador de la red tiene obligaciones respecto de la organización, cuando es empleado; y también, respecto del resto de los empleados, a quienes muchas veces debe controlar.
Ámbito administrativo	El administrador de la red muchas veces es la persona responsable de controlar las bases de datos y otros aspectos que están regulados administrativamente.
Ámbito profesional	En algunos casos, el administrador de la red podría tener responsabilidad con relación al organismo que administre la matrícula profesional.

Tabla 3. Resumen de los diferentes tipos de responsabilidad de un administrador de redes.

RESUMEN

Las tecnologías de la información desafían la interpretación del Derecho. Como su desarrollo está relacionado con el crecimiento de las redes informáticas, el administrador de una red adquiere relevancia. En este capítulo hicimos una introducción a su responsabilidad en los ámbitos civil, penal, laboral, administrativo y profesional.

Capítulo 2

Protección de datos personales y privacidad

Estudiaremos el régimen jurídico de protección de datos personales y la privacidad de las personas.

RedUSERS.com

La intimidad y **el honor de las personas**

Una de las principales consecuencias del avance de la informática y, en particular, de la interconexión de computadoras en red fue la posibilidad de procesar grandes cantidades de información de manera casi instantánea. Esta gran capacidad de cómputo, con un costo relativamente bajo, permitió desarrollar dispositivos informáticos que hoy nos parecen normales, pero que, hace algunos años, hubieran sido impensados, tales como los teléfonos celulares inteligentes (smartphones) o las computadoras táctiles portátiles (tablets).

La ampliación de las capacidades de procesamiento de datos tiene sus ventajas, pero también posee un costado negativo que hace tiempo comenzó a inquietar a los gobiernos y, más precisamente, a las organizaciones que defienden la libertad y los derechos individuales: el procesamiento de datos personales permite realizar perfiles de las personas y avanzar sobre su privacidad de un modo que resulta abrumador. Estos perfiles pueden ser utilizados luego para cometer ilícitos (por ejemplo, para extorsionar), o bien para realizar actividades que, aun cuando son intrínsecamente lícitas –por ejemplo, las actividades de marketing–, pueden implicar una violación de la intimidad y privacidad de las personas en ciertos contextos.

Al advertirse que los datos personales podrían utilizarse para finalidades ilícitas, comenzó a discutirse la necesidad de regular las actividades vinculadas al tratamiento de estos datos. Asimismo, empezó a vislumbrarse la necesidad de reconocer un nuevo derecho para los titulares de los datos personales: el derecho a controlar en todo momento quién tiene los datos, para qué los tiene, y si dichos datos son adecuados y se encuentran actualizados. A esto se lo denomina habitualmente **derecho a la autodeterminación informativa.**

El procesamiento de datos personales permite realizar perfiles de las personas y avanzar sobre su privacidad de un modo que resulta abrumador

Este derecho está íntimamente relacionado con el derecho a la privacidad y al honor de las personas, que se encuentra reconocido en las constituciones de la mayoría de los países occidentales y, asimismo, en diversos tratados internacionales.

A continuación, nos referiremos a los conceptos y principios que rigen en materia de protección de datos personales, y que están presentes, con algunas variantes, en la mayoría de las legislaciones existentes sobre la materia.

Figura 1. **Las redes sociales son una importante fuente de datos personales, que pueden ser tratados para crear perfiles específicos.**

Conceptos básicos de protección de datos personales

Al describir el sistema jurídico de protección de datos personales, tendremos que hacer referencia a ciertos conceptos tales como **dato personal**, **base de datos** y **tratamiento de datos personales**.

Estos conceptos tienen un significado muy específico en el ámbito tecnológico, pero en el jurídico, para evitar inconvenientes al momento de interpretar las normas aplicables, en muchos casos se ha decidido definirlos. Estas definiciones, que están contenidas en las leyes de protección de datos personales, no necesariamente coinciden con las definiciones técnicas, por lo que es importante que el administrador de redes conozca la definición jurídica.

Una de las leyes que más han avanzado en materia de definiciones es la Ley Argentina de Protección de Datos Personales N° 25.326, que fue redactada siguiendo en parte la legislación española, pionera en esta materia.

DERECHO A LA AUTODETERMINACIÓN INFORMATIVA

Es la potestad de toda persona de controlar la información que exista sobre ella en bases de datos. Se ejerce mediante los derechos de acceso, rectificación, supresión o confidencialidad reconocidos en la legislación sobre protección de datos personales.

Figura 2. En la Argentina, la autoridad de aplicación del régimen de protección de los datos personales es la DNPDP (www.jus.gob.ar/datos-personales.aspx).

Es por eso que en esta obra nos referiremos principalmente a los conceptos de la ley argentina, dejando aclarado que podrían existir algunas diferencias en otras legislaciones.

MARCO NORMATIVO DE LA PROTECCIÓN DE LOS DATOS PERSONALES EN DISTINTOS PAÍSES	
Argentina	La protección de los datos personales está regulada en la Constitución Nacional (arts. 19 y 43), la Ley 25.326, el Decreto Reglamentario 1558/2001 y las resoluciones dictadas por la Dirección Nacional de Protección de Datos Personales.
España	El marco normativo está conformado principalmente por la Constitución (art. 18), la Ley Orgánica 15/1999 y diversas Directivas del Parlamento Europeo (como la Directiva 95/46/CE).
México	El marco normativo de México es más reciente: la Ley Federal de Protección de Datos Personales en Posesión de Particulares fue dictada en el año 2010.
Uruguay	La regulación está dada por el art. 72 de la Constitución Nacional, y por la Ley 18.331 de Protección de Datos Personales y Habeas Data, y su Decreto Reglamentario 414/2009.

Tabla 1. Muchos países han avanzado en la regulación de la protección de los datos personales.

DATO PERSONAL

El concepto tal vez más importante es el de **dato personal**, porque este limitará el campo de aplicación de la normativa en la materia. Es decir, al entender a qué clase de información consideramos dato personal, podremos comprender el alcance de la normativa.

Figura 3. **En la Argentina, cualquier información referida a una persona se considera** dato personal.

En este sentido, la ley argentina define el dato personal como "información de cualquier naturaleza, referida a una persona física o jurídica, determinada o determinable".

La definición es muy amplia, dado que comprende **cualquier información**. No es necesario que se trate de información económica: cualquier información sobre una persona es un dato personal para la legislación argentina y, por lo tanto, está protegida. Este mismo criterio amplio es el seguido por la normativa uruguaya, mexicana y española, entre otras.

Una segunda cuestión para tener en cuenta es que la información puede referirse a **personas físicas** o **jurídicas**, lo que significa que también las empresas tienen datos personales. Esto último es destacable porque, en la mayoría de las legislaciones del mundo –entre ellas, la española y la mexicana–, el concepto de dato personal está limitado a las personas físicas, dado que se interpreta que las personas jurídicas no tendrían un honor o privacidad para proteger.

Finalmente, el último punto por destacar respecto del concepto de dato personal es que, en su definición, se hace referencia a personas **determinadas** o **determinables**. Esto significa que no solo constituye un dato personal la información referida específicamente a una persona (por ejemplo, una afirmación como "Juan Pérez tiene un coeficiente intelectual superior al promedio"), sino que también entra en esta

PERSONAS FÍSICAS Y JURÍDICAS

Se consideran personas físicas, naturales o de existencia real a los seres humanos. Por personas jurídicas o de existencia ideal se entiende a las sociedades comerciales, el Estado, y cualquier otra entidad que puede adquirir derechos y obligaciones.

categoría la información referida a un número de personas que no estén identificadas en forma específica, pero que puedan serlo mediante una operación adicional (por ejemplo, una afirmación del estilo "los alumnos de un determinado curso universitario demostraron una inteligencia superior a la media").

Para que se considere que las personas son determinables, debe ser posible identificarlas mediante una operación adicional a la referencia inicial. En el ejemplo que dimos, si alguien consiguiera el listado de los alumnos del curso universitario al que se hace referencia, podría saber con precisión quiénes son las personas que tienen una inteligencia superior a la media.

Este criterio de que el dato personal puede referirse a una persona determinable o identificable es compartido en general por la legislación internacional (por ejemplo, aparece legislado del mismo modo en las normativas española, uruguaya y mexicana).

BASE DE DATOS

Habiendo definido qué se entiende legalmente por dato personal, a continuación nos referiremos al concepto de **base de datos**, que resulta complementario del anterior dado que, para que un dato personal esté protegido, tiene que estar almacenado en una base de datos.

El concepto de base de datos es, quizá, más complejo que el de dato personal, ya que, en este caso, existen definiciones técnicas que tal vez no sean equivalentes a la definición jurídica. Desde el punto de vista legal, y siempre siguiendo las definiciones que contiene la ley argentina, podemos afirmar que se considerará base de datos a cualquier conjunto organizado de datos personales. La clave para el concepto es que exista un **criterio de organización** en el conjunto de datos personales.

La amplitud que presenta esta definición genera inconvenientes interpretativos al momento de aplicarla a ciertos conceptos técnicos, como, por ejemplo, el de una tabla dentro de una base de datos. Es que, desde el punto de vista técnico, una tabla no es, estrictamente, una base de datos; en todo caso, será una parte de ella. Sin embargo, desde el punto de vista jurídico, según la definición que hemos dado precedentemente –y es la que surge de la ley–, una tabla sería una base de datos en sí misma.

LOS DATOS SENSIBLES

Son datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical, e información referente a la salud o a la vida sexual. Salvo autorización legal, está prohibido almacenarlos.

Es importante destacar que, en el régimen argentino, no solo son bases de datos las informatizadas, sino que el concepto abarca también a los tradicionales ficheros que no se encuentran en soporte electrónico. Esto también ocurre con las legislaciones uruguaya, española y mexicana.

TRATAMIENTO DE DATOS PERSONALES

Por último, vamos a referirnos a un tercer concepto que resultará necesario comprender para poder analizar el régimen jurídico de protección de los datos personales y la privacidad: el **tratamiento de datos personales**.

Este concepto tiene gran importancia porque la participación en el tratamiento de los datos personales es uno de los principales aspectos que podrían determinar la responsabilidad del administrador de una red.

En este contexto, podemos adelantar que, al igual que en los casos anteriores, la definición jurídica es muy amplia. En el término tratamiento de datos personales quedan comprendidas todas las operaciones de **recolección**, **almacenamiento**, **modificación** y/o **cesión** de datos personales, por cualquier medio. En estos términos, aunque con algunos matices, se define el tratamiento en las legislaciones argentina, española, mexicana y uruguaya, entre otras.

Figura 4. **También son bases de datos las que se encuentran en el tradicional soporte papel.**

RESUMEN DE CONCEPTOS

Hasta aquí, entonces, describimos los principales conceptos que deben considerarse para comprender el sistema de protección de los datos personales y la privacidad. Dijimos que **cualquier información sobre una persona** es considerada un **dato personal**, que está protegido

EL CONCEPTO LEGAL DE BASE DE DATOS

Para la Ley 25.326, se considera base de datos al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuera la modalidad de su formación, almacenamiento, organización o acceso.

Figura 5. **El concepto de tratamiento de datos personales es muy amplio: abarca su procesamiento, almacenamiento y modificación.**

en la medida en que se encuentre almacenado en una **base de datos**.

También señalamos que el concepto de base de datos es muy amplio, ya que comprende cualquier conjunto de datos personales que esté ordenado según algún criterio.

Por último, vimos que el marco regulatorio prevé que los **datos personales** asentados en **bases de datos** pueden ser **tratados**, y concluimos que el concepto de **tratamiento de los datos personales** también es amplio.

En este contexto, a continuación nos referiremos a los principios que resultan aplicables al tratamiento de los datos personales. Estos principios son los que, interpretados en su conjunto, constituyen el sistema de protección de los datos personales y la privacidad.

Principios aplicables **al tratamiento de los datos personales**

Cuando hablamos de los principios aplicables al tratamiento de los datos personales nos estamos refiriendo a aquellas normas generales que deben ser respetadas para que el tratamiento sea considerado lícito. Es decir, si se tratan datos personales sin respetar estos principios, dicho tratamiento sería **ilegal**.

CONCEPTO LEGAL DE TRATAMIENTO DE DATOS PERSONALES I

El concepto de tratamiento que surge de la ley argentina comprende todas las operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento y modificación de los datos personales.

Si bien en nuestro análisis seguiremos el criterio previsto en la legislación argentina en la materia, estos principios resultan aplicables en prácticamente todos los países que han legislado en materia de protección de datos personales. Con algunas variantes, se trata de principios que incluso son seguidos por países que no tienen una regulación unificada en materia de protección de datos personales, como los Estados Unidos.

PRINCIPIO DE CALIDAD

De acuerdo con el **principio de calidad**, los datos personales que se recolecten e incluyan en una base de datos deben ser **ciertos** y estar **actualizados**.

El responsable o administrador de la base de datos debe velar por que el modo de recolección de dichos datos garantice su fidelidad y veracidad, dado que, en caso de falsedad, tendrá que responder por los daños que pudieran ocasionarse.

Adicionalmente, los datos deben ser actualizados, dado que un dato cierto pero desactualizado puede generar un daño similar al de un dato falso. A modo de ejemplo, un dato personal que puede modificarse y que genera una gran cantidad de consecuencias si no es actualizado es el referido al estado civil. Una persona que en algún momento estuvo soltera podría cambiar su estado a casada y, luego, a divorciada.

También por aplicación del principio de calidad, los **medios de recolección** de los datos personales deben ser **leales**, respetando los derechos de los titulares de dichos datos. Una típica violación a este principio la constituye, por ejemplo, el uso de **cookies** u otros medios de seguimiento de conductas online en forma subrepticia (es decir, sin avisarle al usuario), que es muy habitual en la actualidad en Internet.

El responsable por el cumplimiento de este principio es el **titular** de la base de datos, aunque, como veremos más adelante, la responsabilidad también podría extenderse al administrador de esa base y, asimismo, al administrador de la red en la que se encuentra dicha base de datos.

PRINCIPIO DE FINALIDAD

El **principio de finalidad** en el tratamiento de datos personales está estrechamente vinculado al anterior, y lo complementa.

CONCEPTO LEGAL DE TRATAMIENTO DE DATOS PERSONALES II

El concepto legal de tratamiento también abarca el relacionamiento, evaluación, bloqueo y destrucción de los datos, y en general, su procesamiento y su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

De acuerdo con este, los datos personales que sean recolectados y almacenados en una base de datos deben ser **adecuados** y **no excesivos** para la finalidad de dicha base. Por ejemplo, en la base de datos de usuarios de una red, que contiene habitualmente la información necesaria para validar el acceso y las actividades del usuario, no sería adecuado que el administrador tuviera un campo con la información acerca del salario de dicho usuario. Esto sería completamente excesivo para la finalidad de la base y, por lo tanto, violaría el principio de finalidad.

Este principio tiene también otro aspecto por considerar, y es que una vez cumplida la finalidad para la cual se recolectaron los datos, estos **deben ser destruidos**. Es decir, los datos personales no pueden ser almacenados por más tiempo del necesario para cumplir con la finalidad para la cual fueron recolectados. A modo de ejemplo, los datos personales reunidos para realizar un sorteo deberían destruirse una vez realizado el sorteo (salvo, obviamente, los datos de quien resulte ganador y que sean necesarios para entregar el premio).

Esta regla tiene como importante excepción el caso de que alguna norma legal exija que los datos sean almacenados aun luego de cumplida la finalidad (por ejemplo, el caso de la información comercial, que las empresas deben guardar durante cierto tiempo a los fines probatorios, porque así lo exige la normativa en materia de contratos).

PRINCIPIO DEL CONSENTIMIENTO INFORMADO

Un principio fundamental para la recolección y tratamiento de datos personales es el **principio del consentimiento informado**.

Una vez cumplida la finalidad para la cual se recolectaron los datos, estos deben ser destruidos.

En este sentido, la recolección y tratamiento de datos personales solo será lícita, como regla general, si se cuenta con el consentimiento del titular de dichos datos personales. El consentimiento debe ser brindado en forma **expresa** y **libre**, y **por escrito** o por algún medio que se le equipare.

COOKIES Y OTROS MEDIOS DE SEGUIMIENTO

El uso de cookies y de otros medios para seguir la conducta online de los usuarios resulta potencialmente violatorio del principio de calidad en la recolección de datos personales. Para que sea legítimo, debería advertirse al usuario y requerir su conformidad.

Figura 6. Hay complementos que se añaden a los browsers para bloquear el seguimiento de las conductas online.

Es importante aclarar que el consentimiento informado no puede estar implícito en una declaración del titular de los datos, sino que tiene que ser explícito. Además, el titular de los datos personales debe tener la posibilidad de no brindarlos (este requisito torna inválidos los formularios de Internet en los que el consentimiento para el tratamiento de datos personales aparece como una casilla o checkbox que se encuentra marcada automáticamente).

Por otra parte, la norma establece que debe ser brindado por escrito o por un medio equiparable. Respecto de este último punto, debemos aclarar que en la Argentina existe una Ley de Firma Digital, pero que todavía no ha sido implementada en su totalidad en el ámbito privado. Por lo tanto, el medio equiparable podría ser la utilización de una firma electrónica –que es una categoría similar a la de la firma digital pero que, por faltarle algún elemento de la primera, no brinda las presunciones de autoría e integridad que definen a esta–, o bien otros medios como la grabación de la voz del titular de los datos brindando su consentimiento.

También podrían utilizarse los registros de conexión (logs) del titular de los datos, de donde surja que este ha brindado el consentimiento mediante la aceptación de los términos y condiciones de un sitio o algo similar, pero en este último caso, la prueba podría ser cuestionada.

Adicionalmente, el consentimiento tiene que ser emitido luego de que el titular haya sido informado adecuadamente de los siguientes aspectos:

1. La finalidad para la que serán tratados los datos personales y quiénes pueden ser sus destinatarios.

2. La existencia de la base de datos, y la identidad y domicilio de su responsable.

3. El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga.

4. Las consecuencias de proporcionar los datos personales, de la negativa a hacerlo o de la inexactitud de estos.

5. La posibilidad del titular de los datos personales de ejercer los derechos de acceso, rectificación y supresión ante el responsable de la base de datos.

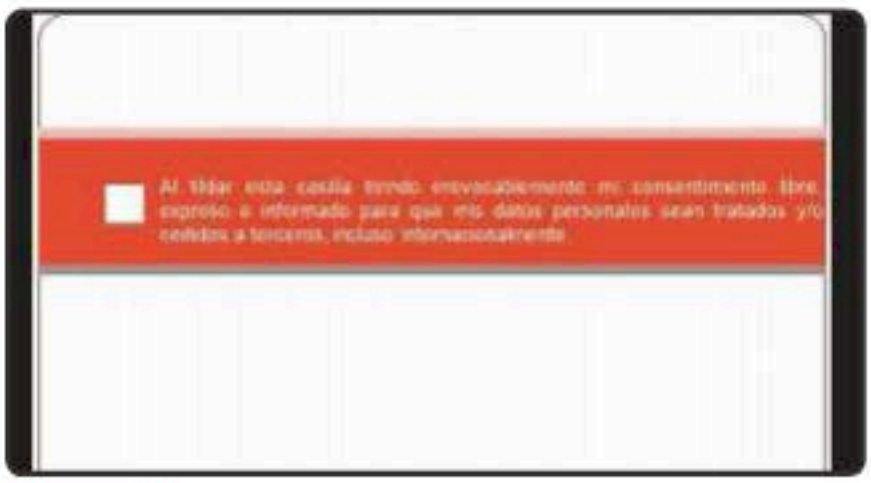


Figura 7. **Ejemplo de un consentimiento informado** inválido.

Esto significa que no sería válido, por ejemplo, que el titular brinde su consentimiento mediante una simple marca en un casillero que diga que así lo hace (sin las explicaciones previas del caso).

Ahora bien, la ley exige que se informe al titular de los datos personales sobre todo lo que describimos anteriormente **de un modo adecuado para su nivel social y cultural**. Esto último es importante porque implica que la descripción no debe tener un lenguaje técnico tal que impida o dificulte su comprensión; debe ser una explicación clara, llana y fácil de comprender por cualquier persona.

Además, debe tenerse presente que el consentimiento es **revocable en cualquier momento**. Es decir, el titular de los datos personales que ha prestado libremente su consentimiento para que sus datos sean incluidos en una base puede, en cualquier momento, retirar dicho consentimiento. En relación a este aspecto, lo que debe tenerse presente es que si la revocación fuera arbitraria, sin una causa razonable, y generase un daño al responsable de la base de datos, posiblemente el titular de los datos personales se vea en la obligación de resarcir dichos daños.

Algunas excepciones al principio del consentimiento informado

A pesar de su importancia para garantizar el derecho a la autodeterminación informativa, el principio del consentimiento informado tiene **importantes excepciones**.

La ley argentina prevé que no es necesario el consentimiento del titular de los datos personales para recabar y/o almacenar sus datos en los siguientes casos:

1. Los datos se obtienen de fuentes de acceso público irrestricto.

2. Se recaban para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal.

LA AUTODETERMINACIÓN INFORMATIVA COMO DERECHO HUMANO

La autodeterminación informativa ha sido considerada en diversas oportunidades por los tribunales como un derecho humano, lo que significa que debe ser reconocida a un nivel incluso mayor que los derechos patrimoniales, como el derecho de propiedad.

Figura 8. De los perfiles en las redes sociales puede obtenerse mucha información personal acerca de sus usuarios.

3. Se trata de listados cuyos datos se limitan a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio.

4. Derivan de una relación contractual, científica o profesional del titular de los datos, y resultan necesarios para su desarrollo o cumplimiento.

5. Se trata de las operaciones que realizan las entidades financieras y de las informaciones que reciben de sus clientes.

A continuación, analizaremos cada una de estas excepciones que terminan desnaturalizando, en cierta medida, la regla general que constituye el principio del consentimiento informado.

Fuentes de acceso público irrestricto

Con relación a la primera de las excepciones, debemos señalar que, por **fuentes de acceso público e irrestricto**, se entiende cualquier fuente lícita de información que no tenga ninguna barrera para su acceso. Tal vez el ejemplo más clásico podría ser la guía telefónica, aunque en la actualidad, sin dudas la fuente más común es Internet. En principio, para tratar los datos personales que se obtengan libremente de Internet, no sería necesario el consentimiento del titular de dichos datos personales. Decimos en principio porque, si el dato personal que figura en Internet proviene de una fuente ilegítima, entonces esto no permitiría su uso sin consentimiento. Pero sí se podrían utilizar sin consentimiento los datos que el titular haya ingresado libremente y no haya protegido, por ejemplo, en las redes sociales.

El ejercicio de funciones propias de los poderes del Estado

La segunda excepción es bastante clara: no se requiere el consentimiento del titular de los datos personales cuando estos son recabados por **el Estado en ejercicio de sus funciones**. Por ejemplo, a los fines de realizar tareas de inteligencia fiscal, las autoridades impositivas pueden realizar cruces de bases de datos

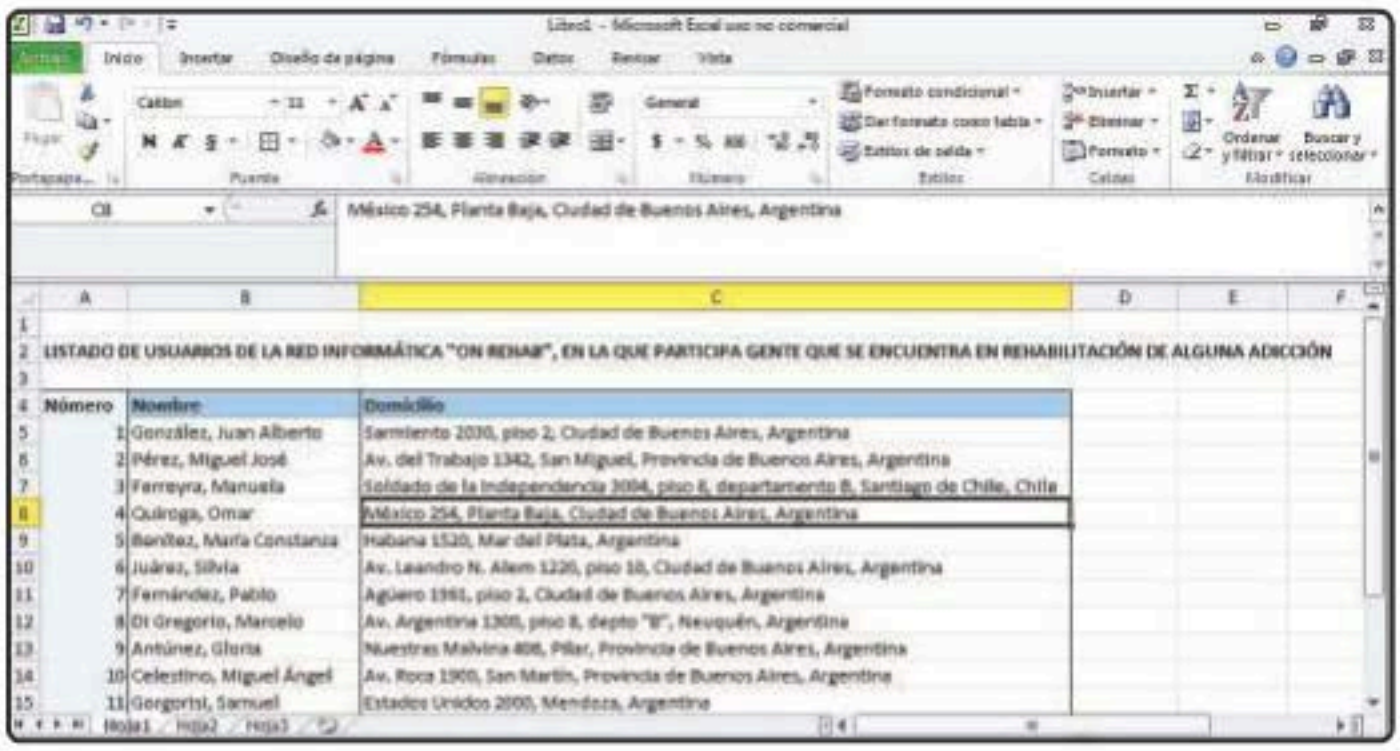


Figura 9. El metadato de que las personas de esta base intercambian experiencias sobre adicciones no está comprendido en la excepción.

con datos personales sin requerir el consentimiento de sus titulares. Desde ya que este tratamiento debe ser efectuado únicamente con la finalidad de ejercer las funciones previstas para el Estado, y respetando los derechos de defensa de los ciudadanos.

También dentro de esta segunda excepción se contempla el caso de que **una ley obligue a tratar determinados datos personales**. Esto ocurre, entre otros casos, con los datos personales de los empleados que deben tratar las empresas. La legislación laboral obliga a las empresas a tratar determinados datos de los empleados, incluso algunos de los cuales son **sensibles** (los vinculados a las enfermedades). Para este tratamiento, no es necesario el consentimiento del empleado.

Categorías específicas de datos personales

En el caso de la tercera excepción a la regla general del consentimiento informado, se trata de **categorías específicas de datos personales cuyo tratamiento no requiere consentimiento**. Estas categorías son únicamente las que mencionamos anteriormente y porque así surgen de la ley. Ahora bien, es muy poco común que dichas categorías aparezcan aisladas en una base de datos, porque casi siempre existirá un metadato que requerirá del consentimiento. Tomando un ejemplo práctico: si

EL DERECHO AL OLVIDO

El derecho al olvido permite que ciertos datos se eliminen de la red, aun cuando cumplan con los principios de protección de datos. Tiene como finalidad evitar que alguna opinión que la persona hubiera emitido en algún momento la persiga toda su vida.

tuviéramos una base de datos de usuarios de una determinada red informática que incluyera solo dos campos, uno para el nombre y el otro para el domicilio, una primera lectura parecería sugerir que nos encontramos en esta excepción al principio del consentimiento informado (porque nombre y domicilio son dos datos que, en sí mismos, no requieren consentimiento para su tratamiento).

Sin embargo, la base de datos también lleva ínsito el metadato de que las personas que aparecen en ella (con sus nombres y domicilios) son usuarios de una determinada red informática, y ese dato personal requiere del consentimiento del titular para ser tratado.

Relación contractual, científica o profesional del titular de los datos

La cuarta excepción está relacionada con ciertas relaciones que pueden existir entre el **titular del dato personal** y el **titular de la base de datos**, que determinan que no sea necesario requerir el consentimiento del primero para el tratamiento de sus datos. En este sentido, la excepción resultará aplicable únicamente para el tratamiento de los datos personales a los fines de dicha relación. En virtud de esta excepción, el administrador de una red puede tratar los datos personales de los usuarios de la red únicamente a los fines de cumplir con sus funciones. Sin embargo, si quisiera utilizarlos para otras finalidades (por ejemplo, para ofrecerles productos o servicios adicionales), requeriría del consentimiento informado.

Entidades financieras y clientes

Por último, la quinta excepción está relacionada con la **actividad bancaria y financiera**, y resulta razonable para que dicha actividad pueda desarrollarse.

Como puede apreciarse, la cantidad de excepciones al principio general del consentimiento informado terminan por desnaturalizarlo, ya que, en la mayoría de los casos, el responsable de la base de datos se encontrará comprendido en alguna de ellas. No obstante, es importante tener en cuenta la existencia de este principio para el administrador de la red, quien seguramente participará en el tratamiento de datos personales de los usuarios.

PRINCIPIOS DE SEGURIDAD Y CONFIDENCIALIDAD

Por último, resta referirnos a dos principios para el tratamiento de los datos personales que son similares y se complementan: los principios de **seguridad** y **confidencialidad**.

De acuerdo con el primero de ellos, el responsable de una base que contiene datos personales **debe garantizar la seguridad** de dicha base de datos. Esto se logra mediante la implementación de medidas de seguridad, tanto físicas como electrónicas o informáticas. Las físicas consisten en el control de acceso a las instalaciones y dispositivos en los que están almacenados los datos. Las electrónicas o informáticas, en cambio, implican el uso de técnicas y programas que impidan que la base de datos pueda ser accedida y copiada por terceros no autorizados.

Figura 10. **Una de las obligaciones del responsable de la base de datos es garantizar la seguridad de la información.**

Respecto del principio de confidencialidad, adicionalmente a las medidas técnicas que mencionamos, adquieren relevancia las medidas jurídicas. Es decir, además de que la base de datos sea segura desde el punto de vista técnico, es necesario que quienes tienen acceso legítimo a ella no divulguen su contenido. Para esto, será responsabilidad del titular de la base de datos suscribir los acuerdos de confidencialidad o los contratos que correspondan para asegurar que, desde el punto de vista legal, todas las personas que accedan a la información estén obligados a guardar secreto.

La transferencia **o cesión de datos personales**

Hasta aquí, hemos analizado el régimen de protección de datos personales, tomando especialmente en consideración los **conceptos** básicos que conforman este régimen y, asimismo, los **principios** que resultan aplicables al tratamiento de los datos personales.

Ahora bien, teniendo en cuenta que el avance de los sistemas informáticos está vinculado a la interconexión en las redes, nos referiremos al régimen jurídico aplicable a la transferencia o cesión de datos personales.

Para esto, haremos una distinción –porque así está previsto en la normativa– entre la **transferencia doméstica** o interna, y la **transferencia internacional.**

LA TRANSFERENCIA DOMÉSTICA O INTERNA DE DATOS PERSONALES

La transferencia doméstica de datos personales ocurre cuando una persona cede datos personales de terceros, que están almacenados en su

MEDIDAS TÉCNICAS PARA GARANTIZAR LA SEGURIDAD Y CONFIDENCIALIDAD DE UNA BASE DE DATOS	
Control de acceso físico	Debe incorporarse un sistema que garantice el control de acceso físico a las instalaciones y sistemas informáticos (por ejemplo, mediante tarjetas magnéticas, dispositivos biométricos, etc.).
Herramientas de seguridad informática	Deben incorporarse sistemas antivirus, firewalls y otros sistemas de seguridad contra posibles ataques externos.
Medidas jurídicas	Deben suscribirse acuerdos específicos de confidencialidad con los empleados y contratistas que tengan acceso a la base de datos. Respecto de los empleados, deben acordarse políticas de uso de los recursos informáticos que garanticen que serán utilizados únicamente para fines laborales.

Tabla 2. **Estas medidas no solo deben ser de índole técnica, sino también jurídica.**

base de datos, a otra persona, siempre **dentro de un mismo país**.

En este caso, resultan aplicables a la cesión los mismos principios que mencionamos para el tratamiento de los datos personales (los principios de calidad, finalidad, seguridad y confidencialidad).

Ahora bien, respecto del consentimiento informado, es importante destacar que el consentimiento para el tratamiento de los datos personales no implica el consentimiento para su cesión. En otras palabras, el hecho de que el titular de los datos personales haya brindado el consentimiento para que sus datos sean ingresados en una base no significa que también haya dado su consentimiento para que dichos datos sean cedidos a terceros.

El consentimiento para la transferencia doméstica debe ser **expreso** y, también, **informado**. En este caso, lo que debe informarse al titular de los datos personales es:

1. A quién serán transferidos sus datos.
2. Cuál es el domicilio de la base de datos a la que serán transferidos.
3. Con qué finalidad se transferirán.
4. Durante cuánto tiempo.

5. Todo otro dato que permita al titular ejercer su derecho de autodeterminación informativa.

Con relación a este tema, en la Argentina existió un caso judicial muy interesante en el cual un tribunal declaró la invalidez de las políticas de privacidad de una importante entidad bancaria en virtud de que, entre otras cosas, en dichas políticas se preveía la posibilidad de que esta entidad pudiera ceder los datos personales de los clientes a otras empresas del mismo grupo, que no estaban claramente identificadas. En dicha oportunidad, el tribunal consideró que una cesión en esos términos resultaría violatoria del régimen de protección de datos personales porque no permitiría al titular tener una idea clara de dónde estarían sus datos, ni por qué motivo serían cedidos. La simple alusión a empresas del grupo, sin identificarlas correctamente, fue considerada como violatoria de los derechos de los titulares de los datos personales.

Figura 11. **Cuando la transferencia se produce dentro de un mismo país, se le aplican los mismos principios que para el tratamiento de datos.**

Excepciones al consentimiento informado para la transferencia de datos personales

Dado que, como dijimos, a la transferencia de datos personales se aplican los mismos principios que al tratamiento, aquí también resultarán de aplicación las excepciones al consentimiento informado.

Por lo tanto, si nos encontramos en algún supuesto en el que no resulte necesario el consentimiento del titular para el tratamiento de sus datos personales, tampoco será necesario dicho consentimiento para la cesión de los datos personales, siempre que esta tenga la misma finalidad que tenía el tratamiento. Por ejemplo, si un banco no requiere el consentimiento de sus clientes para tratar sus datos personales –en la medida en que los trate para el cumplimiento del contrato que han celebrado–, tampoco necesitará el consentimiento del cliente para **tercerizar el tratamiento** en otra empresa. Ahora bien, esta tercerización deberá implicar que la empresa a la que se transfieren los datos los trate del mismo modo en que lo haría el banco, y con las mismas finalidades.

En la Argentina, la ley es muy estricta con relación a las transferencias de datos personales. En efecto, dispone que, en caso de transferencia, sea local o internacional, tanto la empresa que transfiere datos (cedente) como la que los recibe (cesionario) son solidariamente responsables por cualquier incumplimiento de la normativa y daño que pudiera causarse al titular de los datos personales.

TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES

En la transferencia internacional de datos personales, lo relevante es que estos son transferidos hacia un país distinto de aquel en el que se encuentran en primer término.

Esto justifica que el tratamiento de este tipo de transferencias sea, en algunos aspectos, distinto del de las transferencias domésticas. Es que en estos casos, puede ocurrir que el país destino no tenga regulación respecto de la protección de datos personales y, por lo tanto, una vez que los datos personales hayan sido transferidos, sus titulares se vean imposibilitados de ejercer sus derechos.

Es por esto que la legislación argentina, siguiendo en este aspecto lo previsto por la normativa española, estableció una regla muy dura, que implica la prohibición de la transferencia cuando el país destino no es considerado un país seguro.

Ahora bien, ¿cómo saber cuándo un país es seguro a los fines de una transferencia internacional de datos personales? La normativa prevé que una autoridad administrativa, la **Dirección Nacional de Protección de Datos Personales**, está encargada de determinarlo, analizando la legislación del país destino y comparando sus principios con los de la Argentina. Sin embargo, no existen dictámenes hasta la fecha, por lo

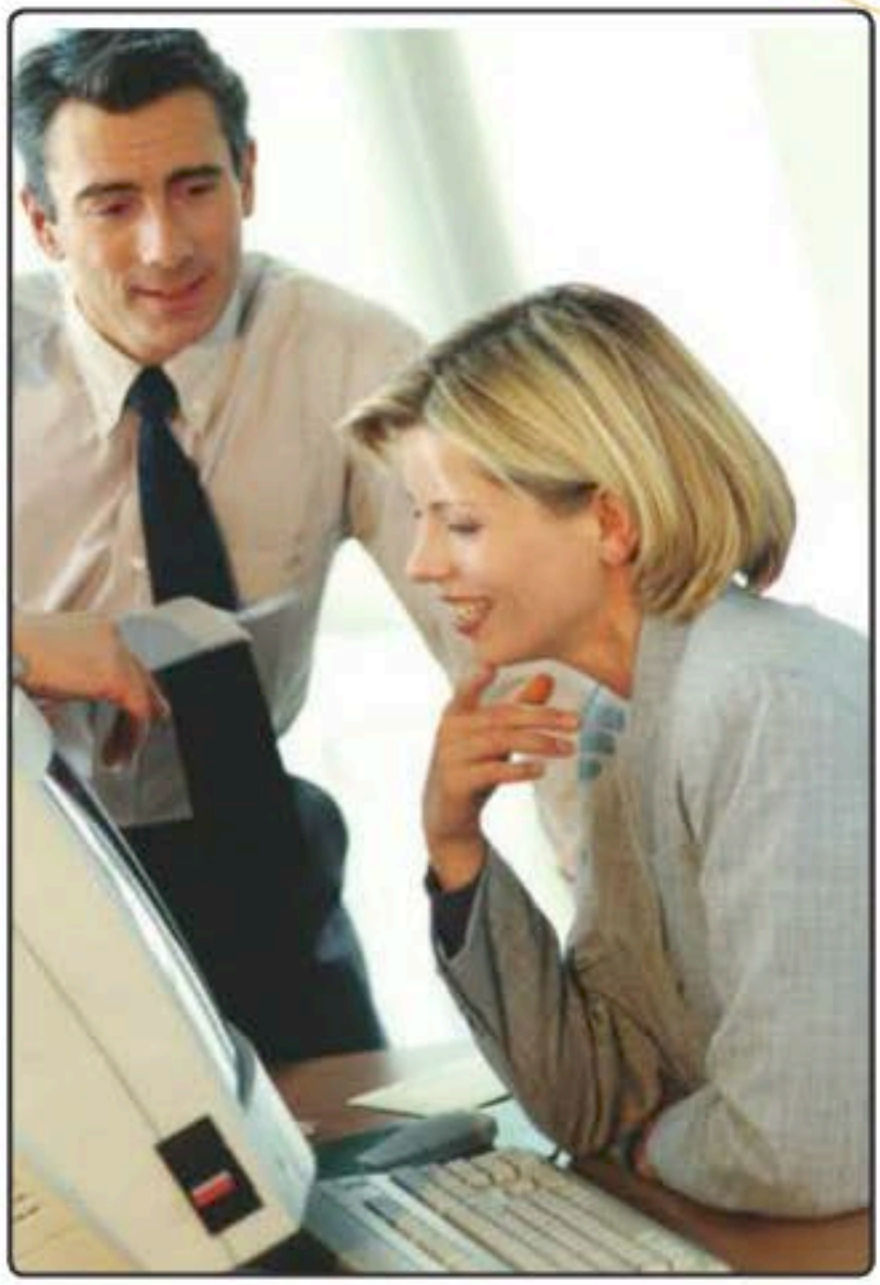


Figura 12. **La responsabilidad debe estar específicamente asumida por las partes en un contrato.**

LA RESPONSABILIDAD SOLIDARIA

Esta significa que todos los obligados deben responder por la totalidad de lo que se debe y que cualquiera puede ser demandado. En el caso de la transferencia de datos personales, cedente y cesionario responden solidariamente por los daños.

Figura 13. **En la Argentina la transferencia internacional de datos personales solo es posible cuando el país destino es considerado seguro.**

que, en principio, no hay una declaración de seguridad para ningún país.

En este contexto, la alternativa para realizar transferencias internacionales de datos está relacionada con la **autorregulación**. La normativa permite a las empresas celebrar acuerdos que prevean la aplicación de los principios de la ley argentina al tratamiento de datos personales en otros países. Estos acuerdos pueden presentarse ante la Dirección Nacional de Protección de Datos Personales y, bajo ciertas condiciones, pueden ser aprobados y permitir instrumentar la transferencia, aun cuando el país destino no fuera seguro.

Responsabilidad por el tratamiento **de datos personales**

El esquema de protección de los datos personales y la privacidad prevé distintos ámbitos de responsabilidad para quienes habitualmente tratan datos personales.

Un primer nivel es el de la **responsabilidad civil**, que tiene como finalidad resarcir los daños que la actividad del tratamiento de los datos personales pudiera generar a los titulares de dichos datos o a terceros.

LOS SERVICIOS CLOUD Y LA TRANSFERENCIA INTERNACIONAL

En la actualidad, existen serias dudas respecto de cómo se resolverán los conflictos legales en los servicios cloud, sobre todo, teniendo en cuenta las prohibiciones o limitaciones que existen en las legislaciones respecto de la transferencia internacional.

Figura 14.
En España, la autoridad de aplicación es la Agencia de Protección de Datos Personales.

En un segundo nivel se encuentra la **responsabilidad administrativa**, cuyo objetivos es castigar el incumplimiento en que pudiera haber incurrido el titular o responsable de la base de datos mediante una sanción que podría implicar, incluso, que deba cesar su actividad profesional.

Por último, en un tercer nivel de responsabilidad por el tratamiento de los datos personales, podemos hacer mención a la **responsabilidad penal**, dado que el marco normativo de protección de los datos personales establece, específicamente, que ciertas conductas son consideradas delito.

A continuación, trataremos brevemente los dos primeros niveles de responsabilidad, dado que lo referido a los delitos vinculados con el tratamiento de los datos personales será abordado en el Capítulo 3 de este libro.

RESPONSABILIDAD CIVIL

Tal como señalamos en el Capítulo 1, la responsabilidad en el ámbito civil tiene como principal finalidad la reparación a quien ha sido dañado. No se busca tanto el castigo de quien cometió el daño, sino más bien, la reparación de dicho daño (el castigo, en todo caso, se perseguirá en el ámbito penal o administrativo).

En el caso del tratamiento de datos personales, los daños pueden generarse por:

EL SPAM Y LOS DATOS PERSONALES

Dado que la dirección de correo electrónico es un dato personal, la actividad de los spammers puede ser cuestionada por violar la normativa de protección de datos personales. En la Argentina hubo una condena basada en la ley de datos.

1. El incumplimiento de alguno de los principios que surgen de la normativa, que ocasione un daño (por ejemplo, la filtración de información confidencial debida a una falla en el deber de seguridad del titular de la base de datos).

2. Algún incumplimiento derivado de la transferencia de los datos personales, sea doméstica o internacional.

Daños por incumplimiento de la normativa

Si los daños se generan como consecuencia del incumplimiento de alguno de los principios que rigen en materia de protección de datos personales, el titular de la base de datos y, eventualmente, el administrador de dicha base, si hubiera sido el responsable de la acción dañosa, deberán responder ante el titular de los datos personales por el daño ocasionado. Es importante adelantar que, como mencionaremos más en detalle en el Capítulo 5 de este libro, los daños deben ser debidamente cuantificados y tener un correlato con el padecimiento real que hubiera tenido el titular de los datos personales.

Si el titular de la base de datos fuera una empresa, de acuerdo con el régimen general de responsabilidad civil, deberá responder por las acciones de sus empleados. Por lo tanto, si la acción que desencadenó el daño fue de algún empleado, quien responde frente al titular de los datos personales es la empresa (sin perjuicio de que después, en determinadas circunstancias, esta pueda reclamar a su empleado por los daños que tuvo que afrontar).

Para determinar el alcance del deber de reparar, habrá que analizar la relación jurídica existente entre el responsable de la base de datos y el titular de los datos personales, cómo fue que el responsable de la base obtuvo los datos personales, a qué se debió el incumplimiento con la normativa, etcétera. Además, en caso de existir un contrato entre el responsable de la base de datos y el titular de los datos personales, deberá analizarse si dicho contrato contiene alguna cláusula limitativa de la responsabilidad y, en su caso, si dicha cláusula es válida.

Daño por incumplimiento en la transferencia de datos

En el segundo caso, es decir, si los daños se generasen como consecuencia o con relación a una transferencia de datos personales, sea local o internacional, la normativa establece

EL REGISTRO DE LAS BASES DE DATOS

En general, las legislaciones exigen que las bases de datos que contienen datos personales sean registradas ante la autoridad de aplicación. Este registro no implica la entrega de los datos que obran en la base, sino solo la declaración de su existencia.

expresamente que todas las personas que hubieran participado en la transferencia deben responder en forma solidaria (cualquier de ellos podría ser demandado por la totalidad de los daños ocasionados). En este caso, será algo más difícil limitar la responsabilidad de los participantes de la transferencia, porque la realidad es que la normativa no alienta la transferencia de datos personales, sino todo lo contrario.

RESPONSABILIDAD ADMINISTRATIVA

En el ámbito administrativo, la responsabilidad del titular de la base de datos que ha incumplido con alguno de los principios que conforman el régimen de protección se hace efectiva frente a la autoridad de aplicación de la Ley de Protección de Datos Personales.

En este caso, la responsabilidad no tiene como finalidad resarcir al damnificado –como ocurre en el ámbito civil– sino más bien castigar al infractor por no haber cumplido con la norma. Este castigo, a su vez, no tiene el nivel de gravedad de un castigo penal, porque la violación de la normativa podría no implicar la comisión de un delito penal, como veremos más adelante en el siguiente capítulo de esta obra.

El titular de la base de datos que ha violado alguna de las normas que rigen el sistema de protección de los datos personales puede ser sancionado por la autoridad de aplicación, aun cuando no se hubiera causado un daño efectivo al titular de los datos personales. Es que, en este ámbito, no se persigue la reparación ni el castigo por el daño ocasionado, sino que la finalidad de la sanción es que el infractor **adecue su conducta a la normativa**.

Las sanciones que se pueden imponer en el ámbito administrativo consisten en:

1. Apercibimientos: son como llamados de atención.

2. Multas: son sanciones pecuniarias.

3. En caso de gravedad o de reiteración en los incumplimientos de la normativa, la autoridad de aplicación podría determinar la cancelación de la base de datos del infractor, impidiéndole continuar su actividad profesional.

Con relación a las personas que pueden ser sancionadas en este ámbito, resultan de aplicación los

SANCIONES ADMINISTRATIVAS Y SU NECESARIA REVISIÓN JUDICIAL

Las autoridades de aplicación de la normativa de protección de datos personales tienen facultades para aplicar sanciones. No obstante, estas sanciones deben ser revisadas por un juez para garantizar el derecho de defensa de los sancionados.

criterios que señalamos para el caso de la reparación civil. Es decir, en primer lugar, el responsable primario será el titular o responsable de la base de datos que no ha cumplido con la normativa, pero si hubiera existido transferencia de datos personales, también serán responsables los que hubieran participado de la cadena de transferencia.

RESPONSABILIDAD PENAL

El último ámbito de responsabilidad por el tratamiento de datos personales es el penal. En este caso, nos encontramos ante conductas que, más allá de la violación de los principios que rigen el sistema de protección de datos personales, constituyen un delito penal. Por lo tanto, en este ámbito la responsabilidad es personal (no hay posibilidad de que exista responsabilidad solidaria en materia penal), y cada persona responde por sus propios actos.

A pesar de que en el ámbito del derecho penal puede solicitarse también una reparación civil, la sanción habitual en este ámbito es la pena privativa de la libertad. Es decir, en caso de que se comprobase la comisión de un delito de los previstos en el régimen de protección de datos personales, la persona que lo hubiera cometido podría ser condenada a prisión.

El régimen de protección de datos personales prevé diversas figuras delictivas, con distintas penas según la gravedad del delito. Estas figuras serán analizadas en el próximo capítulo, en el que abordaremos los temas penales.

RESUMEN

El marco regulatorio de protección de datos personales contiene diversas definiciones y principios que, interpretados conjuntamente, constituyen un régimen complejo y muy preciso de protección. El incumplimiento de estos principios genera responsabilidad en diversos ámbitos.

Capítulo 3

Delitos informáticos

Analizaremos las conductas que,
por su grado de afectación a los valores
sociales, merecen un castigo penal.

RedUSERS.com

Los delitos **informáticos**

En este capítulo analizaremos los **delitos informáticos**, conductas que, por el grado de afectación a los valores de la sociedad, son castigadas con las máximas penas que prevén los sistemas jurídicos (habitualmente, la privación de la libertad de quien los comete).

Para esto, nos adentraremos en algunos conceptos del **Derecho Penal**, que, como vimos, es la disciplina a la que se recurre como última instancia en el sistema jurídico para proteger los valores más preciados de una sociedad.

Es importante destacar que no todas las conductas ilegítimas son consideradas delitos, sino solo aquellas que cumplen con los recaudos necesarios para ser tomadas como tales. Existe una gran cantidad de conductas reprochables, y hasta ilegítimas en el ámbito del Derecho Civil, pero que no son delitos penales. A modo de ejemplo, podemos mencionar el incumplimiento de las obligaciones de un contrato, que, salvo ciertas excepciones, no constituye un delito penal en la mayoría de las legislaciones, sino solo un acto ilegítimo en el ámbito civil.

Concepto **de delito penal**

Dado que el **delito informático** es una categoría de delito penal, resulta necesario, ante todo, comprender qué es un **delito penal**. En este sentido, podemos decir que un delito penal es una **acción típica antijurídica y culpable**.

Esta es la definición clásica que se utiliza en la teoría del delito y resulta aplicable, con algunas variantes, en los distintos países en que rige el derecho de fuente continental europeo (no así

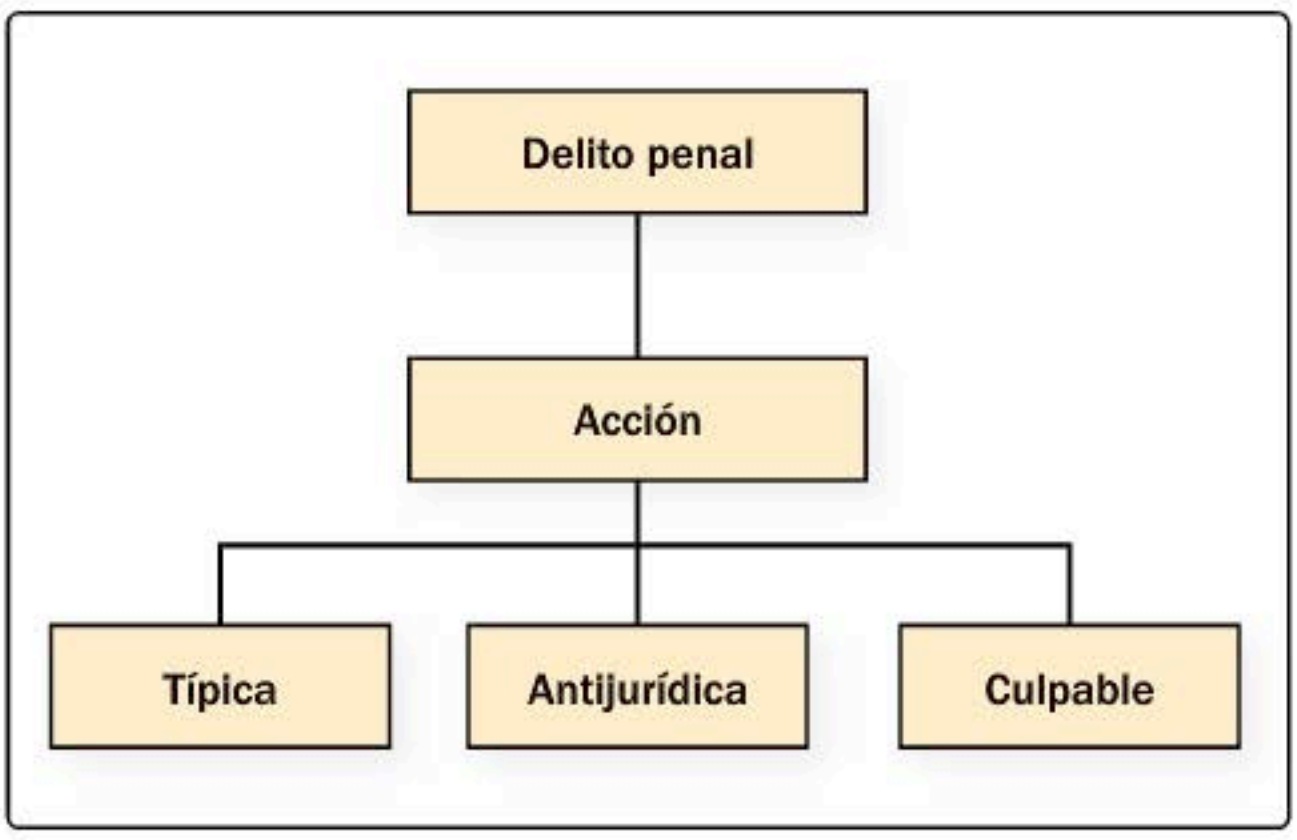


Figura 1. **Los jueces penales deben analizar si una conducta se adecua a lo previsto en un tipo penal.**

en el régimen del **Common Law**, cuyas diferencias mencionamos en el Capítulo 1 de esta obra).

A continuación, explicaremos cada uno de los elementos que componen un delito penal, dejando aclarado que todos deben estar presentes para que una conducta sea considerada como tal. Por lo tanto, cuando un juez evalúa un hecho ilícito, lo que verifica es la adecuación de la conducta a estos elementos. Si se adecua, estamos ante un delito penal; mientras que en caso contrario, la conducta no será punible en el ámbito penal (lo que no impide que quien cometió el hecho deba reparar los daños en el ámbito civil).

PRIMER ELEMENTO DE LA TEORÍA DEL DELITO: LA ACCIÓN

El primer elemento que debe estar presente en un delito penal es la **acción**, entendida como un **acto humano voluntario**. Este hecho nos indica que, sin la participación de una persona física, no hay delito penal.

Ahora bien, esta acción humana debe ser **voluntaria**, por lo que no habrá delito cuando la persona haya cometido la acción sin voluntad. Un ejemplo típico es el de quien se encuentra en un recital y, al producirse una avalancha de gente, en virtud de la fuerza incontenible que esta tiene, lesiona a quien está por delante. En este contexto, aunque la persona lesionada tuviera heridas graves, en principio, no podría imputarse delito penal alguno a quien la lesionó, dado que no hubo voluntad de hacerlo (en el ejemplo, tal vez habría responsabilidad penal de quienes iniciaron o incitaron a la avalancha).

Por último, debemos señalar que la acción requerida para que exista un delito penal puede ser positiva o negativa. En el primer caso, el delito consistirá en **hacer algo**, mientras que en el segundo se trata de los **delitos de omisión**, que consisten en un **no hacer** algo que genera la consecuencia disvaliosa. Los delitos de omisión son muy poco frecuentes, y no están presentes en el ámbito del Derecho Informático, en el que todos los delitos son de acciones positivas.

SEGUNDO ELEMENTO DE LA TEORÍA DEL DELITO: LA TIPICIDAD

Como vimos, para constituir un delito penal, la acción debe ser típica. Ahora bien, ¿qué significa esto? Los **tipos penales** son las normas específicas del Derecho Penal mediante las cuales se describe el delito penal. En otras palabras,

LAS PERSONAS JURÍDICAS NO COMETEN DELITOS PENALES

Las personas jurídicas no cometen delitos ni pueden ser castigadas con pena privativa de la libertad (no se podría encarcelar a una sociedad anónima). Son sus administradores quienes responden personalmente por las acciones ilegítimas de estas.

solo son delitos penales las conductas que están descriptas en tipos penales. Habitualmente, los tipos penales están contenidos en una ley, que suele denominarse Código Penal.

Contrariamente a lo que podría imaginarse, los tipos penales no están redactados en términos de prohibición, sino que describen conductas añadiendo la consecuencia penal (sanción) para quien las cometa. A modo de ejemplo, el tipo penal genérico para el delito de homicidio podría formularse del siguiente modo: "Se aplicará prisión de x a xx años al que matare a otro". Como puede apreciarse, el tipo contiene un **verbo típico**, que nos indica cuál es la acción (en este caso, matar), y la pena que corresponde a dicha acción (en este caso, una cantidad de años de prisión).

Entonces, podemos resumir este segundo elemento —la tipicidad— en el análisis que debe realizarse de la acción para verificar que se adecue a un tipo penal. Si la acción no está prevista en un tipo penal, por más disvaliosa o injusta que pueda parecer, no será un delito penal. Es importante destacar que **la adecuación debe ser perfecta**, porque en el ámbito del Derecho Penal no puede utilizarse la analogía para interpretar un tipo penal (a modo de ejemplo, si un tipo penal sancionara la conducta de quien atacase a otro mediante el uso de un cuchillo, no podría interpretarse que ha cometido esa acción quien atacase con otro elemento cortante distinto de un cuchillo).

TERCER ELEMENTO DE LA TEORÍA DEL DELITO: LA ANTIJURIDICIDAD

Hasta aqui, entonces, hemos visto que, para que una conducta sea considerada delito penal, debe ser una **acción humana voluntaria** y, además, debe estar contenida en un **tipo penal**.

Ahora bien, además de lo expuesto, la conducta debe ser **antijurídica**. Esto significa que debe ser contraria al ordenamiento jurídico en su conjunto. Es decir, podrían existir conductas que, a pesar de estar contenidas en un tipo penal, no sean antijurídicas por estar permitidas por alguna otra norma del sistema jurídico.

Tal vez el ejemplo más claro sea el de la **legítima defensa**. En este caso, estaríamos ante una **acción** (por ejemplo, la lesión a una persona), **típica** (porque lesionar a otro está contenido en un tipo penal), pero que en este caso puntual **no sería antijurídica** si quien la lleva a cabo lo hace para defender su vida, amenazada por quien resultó lesionado.

EL CÓDIGO PENAL

Todos los delitos deberían de estar contenidos en el Código Penal, porque esto brindaría certeza y seguridad jurídica. No obstante, en la actualidad, la tendencia es que las leyes penales especiales también tipifiquen delitos por fuera del Código Penal.

Por lo tanto, al llegar a este nivel del análisis, el juez debe evaluar si la conducta –que, en este punto, ya sabe que se adecua a un tipo penal– es antijurídica o, por el contrario, podría estar autorizada por alguna norma del sistema jurídico (como el caso de la legítima defensa). Si llegase a la conclusión de que la conducta no es antijurídica, entonces no habrá delito penal.

CUARTO ELEMENTO DE LA TEORÍA DEL DELITO: LA CULPABILIDAD

Resta analizar el último elemento de la teoría del delito, en el que la evaluación no se centrará en los aspectos objetivos de la conducta sino, más bien, en la intención de quien la cometió.

En efecto, en el ámbito de la culpabilidad, lo que se analiza es si la persona que realizó la conducta típica y antijurídica actuó con intención de hacerlo, o si lo hizo por impericia, negligencia o imprudencia. Si lo hizo con intención, estaremos ante un obrar **doloso**; mientras que si lo hizo por impericia, negligencia o imprudencia, nos encontraremos ante un obrar **culposo**. Las consecuencias en uno y otro caso serán distintas, porque es evidente que no puede castigarse del mismo modo a quien realiza un acto deliberadamente, que a quien lo hace por

Figura 2. **En el delito doloso, la persona tiene la intención de realizar la acción y sabe cuál es la consecuencia.**

negligencia. Consecuentemente, las penas son diferentes en el caso de los **delitos dolosos** y en el de los **delitos culposos**.

Ahora bien, no todos los delitos admiten la comisión dolosa y culposa. En otras palabras, hay delitos que solo pueden ser cometidos cuando hay intención; por lo tanto, no existiendo intención, aunque la conducta y la consecuencia sean la misma, no hay delito penal.

Este es el caso de los **delitos informáticos**, en los cuales, en términos generales, siempre se requerirá el dolo de la persona que los comete.

LOS ELEMENTOS DEL TIPO PENAL

El tipo penal contiene un verbo típico (que permite identificar la conducta reprochable), más la individualización de la pena que corresponde a esa conducta. Adicionalmente, pueden preverse agravantes o atenuantes de la pena.

RESUMEN DE LA TEORÍA DEL DELITO

Como dijimos al comenzar este capítulo, ante un determinado hecho, el juez debe analizar si existe una **acción típica, antijurídica y culpable**. En el cuadro que presentamos a continuación, procuramos resumir los aspectos más relevantes de cada una de estas definiciones, a modo de repaso de lo expuesto hasta el momento en este capítulo.

CONCEPTOS PRINCIPALES DE LA TEORÍA DEL DELITO	
Acción	Tiene que ser un acto humano voluntario. Puede consistir en una acción positiva (algo que se hace) o negativa (una omisión).
Típica	La acción debe estar incluida en un tipo penal, una norma que establece que esa acción es un delito penal. La adecuación de la acción a lo que se encuentra previsto en el tipo penal debe ser exacta, dado que no se pueden realizar interpretaciones analógicas en el ámbito del Derecho Penal.
Antijurídica	La acción típica debe contravenir el orden jurídico en general, lo que significa que no debe estar permitida por ninguna norma (por ejemplo, como ocurriría en el caso de la legítima defensa, en el cual una acción típica podría estar permitida en ciertos casos).
Culpable	Los delitos pueden ser dolosos (la acción debe realizarse con intención) o culposos (la acción se realiza mediando negligencia, impericia o imprudencia). No todos los delitos admiten las dos formas de comisión. En el caso de los delitos informáticos, en general se trata de delitos que únicamente admiten la comisión dolosa.

Tabla 1. Estos conceptos son los pasos fundamentales que deben revisarse para determinar si estamos ante un delito penal.

LAS CATEGORÍAS DEL DOLO

El dolo puede ser directo, indirecto o eventual. El primero es el más grave, porque el autor comete la acción buscando el resultado. En los otros, si bien hay intención, el resultado no es necesariamente el buscado (indirecto) o al autor no le importa (eventual).

Principios y reglas **de interpretación del ámbito penal**

Dado que el Derecho Penal protege los valores más preciados de la sociedad y, por lo tanto, las sanciones que impone son las más graves del sistema jurídico, existen ciertos principios y reglas de interpretación que son propios de esta disciplina jurídica.

Estos principios y reglas de interpretación tienen por finalidad regular el alcance de los poderes del Estado en las causas penales, al garantizar el derecho de defensa de las personas que pueden ser imputadas en dichas causas.

A continuación, repasaremos solo aquellos que resultan relevantes para comprender cómo deben interpretarse los delitos informáticos, que analizaremos más adelante en este capítulo.

LOS PRINCIPIOS DE LEGALIDAD Y DE IRRETROACTIVIDAD DE LA LEY PENAL

Hay dos principios que están estrechamente vinculados y se refieren a los **tipos penales**, que, como vimos, son las normas que describen las conductas delictivas.

En este sentido, de acuerdo con el principio de **legalidad**, los tipos penales deben ser establecidos por leyes sancionadas por el Poder Legislativo. Es decir, como regla general, no se podrían establecer tipos penales mediante decretos u otras normas distintas de leyes. Este principio garantiza que solo serán consideradas como delitos penales aquellas conductas que la sociedad –a través de sus representantes designados en el Poder Legislativo– considere como las más graves en un momento dado, con independencia de quien esté ocupando el Poder Ejecutivo del Estado en dicho momento.

Este principio ha sido criticado porque, habitualmente, el procedimiento para sancionar una ley es complejo y demora algún tiempo. Y hasta tanto sea dictada la ley que establece un determinado tipo penal, la conducta sancionada por ese tipo penal no será delito.

Ahora bien, el principio de legalidad se complementa con otro principio, que es el de la **irretroactividad** de la ley penal. Según este, las leyes penales siempre regirán hacia el

LA CULPA EN EL ÁMBITO PENAL

La negligencia consiste en hacer menos de lo que se debe (por ejemplo, no tomar ciertos cuidados), la imprudencia en hacer más de lo que se debe (como exceder la velocidad permitida) y la impericia está asociada a un conocimiento profesional (por ejemplo, médico).

Figura 3. **Según el principio de irretroactividad, los delitos siempre regirán para el futuro.**

futuro. Esto es muy razonable, porque en caso contrario, se generaría inseguridad jurídica (no tendríamos certeza acerca de si las acciones que realizamos hoy serán consideradas como delitos mañana).

De acuerdo con el principio de irretroactividad, la ley que estableció que una determinada conducta es un delito debe estar vigente al momento de cometerse el hecho.

Sin embargo, el principio de irretroactividad tiene una importante excepción: la **aplicación de la ley penal más benigna**. Si se está juzgando un delito y, mientras tramita el proceso, el legislador decide derogar ese delito (mediante una ley que disponga una modificación en el Código Penal), entonces el delito ya no podrá ser perseguido, y el proceso que está en trámite deberá suspenderse. Del mismo modo, cualquier persona que estuviera cumpliendo una condena en virtud de un delito que hubiera sido derogado debería ser puesta en libertad de inmediato.

LA PRESUNCIÓN DE INOCENCIA Y EL PRINCIPIO IN DUBIO, PRO REO

Estos dos principios constituyen garantías fundamentales de las personas, que están presentes en prácticamente todas las constituciones.

La **presunción de inocencia** implica que, por regla general, la culpabilidad debe demostrarse. No es el imputado de un delito quien debe probar que no lo ha cometido, sino que es quien lo acusa (habitualmente, un fiscal o un juez dependiendo del sistema penal) quien debe probar que es culpable. Para esto, debe destruir la presunción de inocencia. Se trata aquí de una garantía fundamental para cualquier sociedad

CASO DE HACKING EN LA CORTE SUPREMA DE JUSTICIA

En 1998, el sitio web de la Corte Suprema de Justicia de la Argentina fue hackeado. Los autores fueron descubiertos pero no fueron condenados penalmente, porque la conducta no se encontraba tipificada en una norma penal. Por lo tanto, no había delito penal.

moderna, que permite a las personas tener la certeza de que nadie las privará de su libertad arbitrariamente (para hacerlo, será necesario llevar adelante un proceso penal en el cual se demuestre que se ha cometido un delito, y tal demostración requerirá de prueba para derribar esta presunción de inocencia).

Ahora bien, además de la presunción de inocencia, existe otro principio, conocido por su denominación latina **in dubio, pro reo**, que significa, **en caso de duda, debe estarse a favor del imputado**. De acuerdo con este principio, para condenar a alguien por la comisión de un delito, el juez debe tener certeza de que esa persona lo cometió. En caso de que el juez tenga dudas, no puede condenar. La certeza debe provenir de las pruebas que se produzcan en la causa, las cuales deben llevar, inequívocamente, a la certeza de que la persona imputada es quien ha cometido el acto delictivo.

LA INTERPRETACIÓN RESTRICTIVA DE LA LEY PENAL

A diferencia de lo que ocurre en otras disciplinas jurídicas, la interpretación de las normas en el ámbito penal es muy estricta, y quedan prohibidas la **interpretación analógica** y la **interpretación extensiva**.

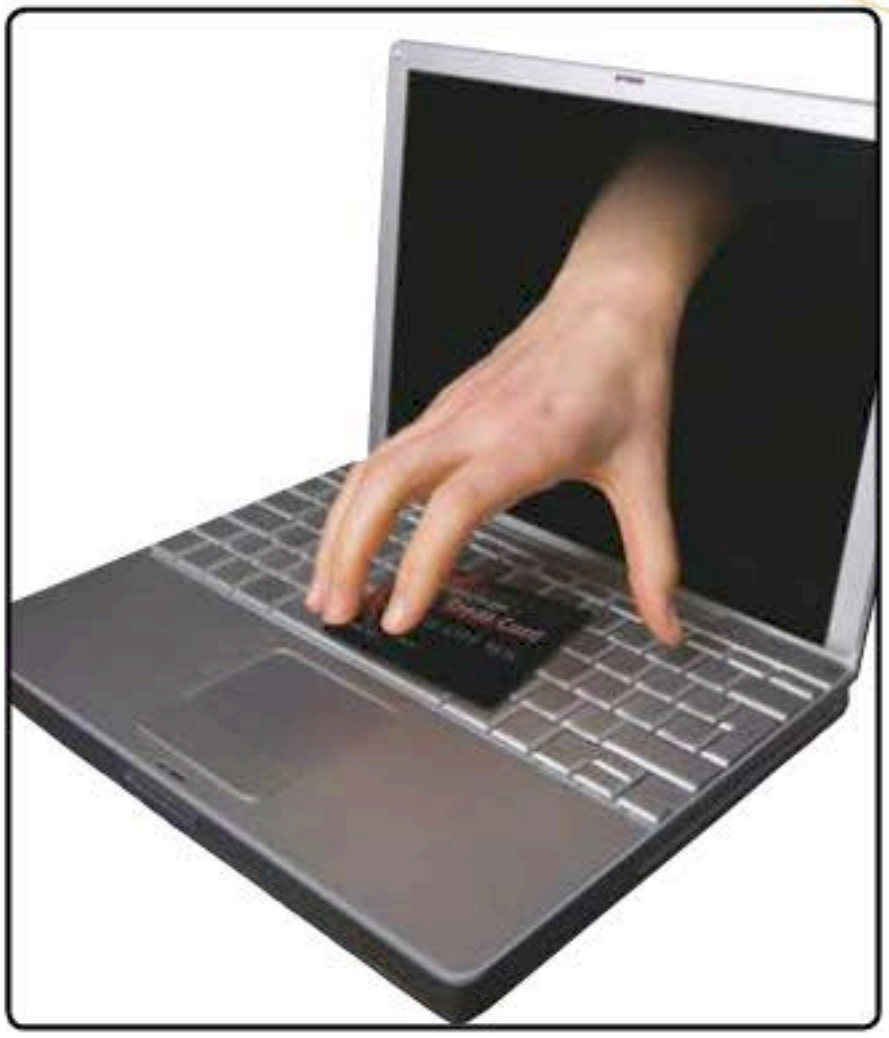


Figura 4. La prueba de los delitos informáticos debe producir certeza en el juez para que exista condena.

Por ejemplo, si un tipo penal estableciera: "Será penado con prisión de 3 a 5 años quien destruyera información almacenada en un archivo digital", no podría interpretarse que comete ese delito quien destruye información almacenada en un archivo tradicional –no digital–, porque sería una interpretación analógica. Y tampoco podría interpretarse que comete este hipotético delito quien **copiase**

LA PRUEBA DE LOS DELITOS INFORMÁTICOS

En el ámbito de los delitos informáticos, a veces resulta difícil destruir la presunción de inocencia con pruebas que son meros indicios de que fue el imputado quien cometió la acción (por ejemplo, por su vinculación con una dirección IP).

información almacenada en un archivo digital, porque en este caso estaríamos ante un supuesto de interpretación extensiva.

Estas reglas de interpretación de la ley penal también tienen como finalidad brindar seguridad jurídica y permitir que cualquier persona, con solo leer el Código Penal, pueda saber con certeza qué conductas son consideradas delitos penales y, así, evitar cometerlas.

Como puede apreciarse, estas reglas resultan muy razonables en el ámbito físico, pero pueden complicar enormemente la interpretación de los delitos cometidos por medios informáticos.

A modo de ejemplo, podemos comentar un caso que llegó a los Tribunales en la Argentina, referido a un supuesto **hurto** de correos electrónicos. En el caso, una persona denunció en un expediente judicial que otra había ingresado en su casilla de correo electrónico y le había hurtado ciertos correos. Es importante recordar que el delito de hurto consiste en el desapoderamiento de una cosa sin violencia (si hubiera violencia, estaríamos ante el delito de **robo**).

En este contexto, dado que la acción de quien habría cometido el supuesto hurto consistió en acceder a la casilla y reenviarse ciertos correos electrónicos, pero sin borrarlos de la fuente, el Tribunal consideró que no había delito. Esto porque, según palabras del Tribunal, no había existido desapoderamiento, dado que la realidad es que los correos electrónicos supuestamente hurtados seguían estando en la casilla original.

Figura 5. La aplicación de los criterios de interpretación penal dificultan la persecución de conductas del ámbito virtual.

Desde el punto de vista de la aplicación de las normas que rigen la interpretación de la ley penal, la opinión judicial fue, sin dudas, correcta. Sin embargo, evidencia que la aplicación de las tecnologías de la información genera desafíos para la ley penal, que son difíciles de resolver, salvo mediante normas penales que sean dictadas teniendo especialmente en cuenta las nuevas tecnologías.

EL DERECHO DE DEFENSA

Por último, nos referiremos al **derecho de defensa**, que es otro principio constitucional aplicable en el ámbito penal.

Según este principio, toda persona tiene derecho a ser escuchada por el tribunal que la juzgue, a ofrecer y producir la prueba que considere necesaria para su defensa, y a controlar la prueba que sea producida por el tribunal y/o por el fiscal y/o por la parte contraria. La prueba que se produzca en una causa penal en violación a

este principio será **nula**, y no podrá ser tenida en cuenta para una eventual condena.

En el ámbito del Derecho Informático, se plantean muchas situaciones en las cuales la falta de cuidado en el manejo de la prueba determina que, luego, sea nulificada por el tribunal. Un ejemplo típico ocurre con el secuestro de computadoras, que, en muchos casos, se realiza sin tomar las medidas adecuadas, tales como el precintado de los equipos secuestrados (lo que implica tapar todos los puertos de entrada/salida de información para evitar que el imputado pueda alegar que la información que contenía la máquina fue modificada durante o luego del secuestro).

RESUMEN DE CONCEPTOS BÁSICOS DEL DERECHO PENAL

Hasta aquí, hemos repasado algunos conceptos básicos del Derecho Penal, que nos permitirán analizar y comprender el significado y las categorías de los delitos informáticos.

En este sentido, hemos mencionado que los **delitos informáticos** son una categoría especial de **delitos penales**, y que los delitos penales son **acciones típicas, antijurídicas y culpables**.

Asimismo, hemos señalado que, para que una acción pueda ser considerada como un delito penal, debe adecuarse de un modo perfecto al tipo penal, porque, en caso contrario, estaríamos ante una conducta que podría ser reprochable pero que no sería delito penal.

Por último, repasamos ciertos principios que resultan aplicables al Derecho Penal y que limitan o regulan el modo en que deben aplicarse las normas penales. En virtud de estos principios, por ejemplo, podemos afirmar que, para condenar a una persona por un delito penal, habrá que destruir su **presunción de inocencia**, y esto deberá hacerse

Figura 6. La correcta manipulación de la prueba es fundamental, para evitar planteos de nulidad de la defensa.

LA CADENA DE CUSTODIA DE LA PRUEBA

El imputado debe poder saber quién manipuló la prueba en todo momento. Por ejemplo, en el caso del secuestro de un CD con información, debe existir un documento que establezca quién lo tuvo en sus manos hasta que llegó al depósito judicial.

mediante la producción de **prueba legítima** (es decir, prueba cuya producción pueda ser debidamente controlada por la persona acusada).

En este sentido, también mencionamos que, por aplicación del principio **in dubio, pro reo**, la prueba debe ser concluyente, porque si el tribunal tiene dudas acerca de si el imputado cometió o no el delito que se le imputa, debe emitir su fallo a favor del imputado.

Teniendo presentes estos conceptos, a continuación analizaremos algunos de los delitos informáticos más comunes.

Los denominados **delitos informáticos**

Desde hace ya tiempo que, en el ámbito del Derecho Penal, se comenzó a hablar de una categoría especial de delitos, a la que genéricamente se denominó **delitos informáticos**.

Sin embargo, al intentar definir estos delitos mediante una característica o rasgo común, no había un acuerdo pleno en la doctrina jurídica. Es que, por un lado, estaban quienes sostenían la teoría de que los delitos informáticos son **delitos penales tradicionales**, pero cometidos a través de medios informáticos. Es decir, para esta primera posición, lo definitorio para esta categoría delitos sería el medio comisivo, y no, las conductas en sí. Se trataría de las mismas conductas que estaban previstas en los códigos penales tradicionales, pero cometidas a través de medios informáticos. Siguiendo esta teoría, por ejemplo, la sustracción ilegítima de dinero de una cuenta bancaria por Internet sería un hurto informático.

Ahora bien, como vimos, en el ámbito del Derecho Penal existen importantes restricciones para la interpretación de las normas, que se relacionan con la imposibilidad de realizar analogías o extensiones. Fundada en estas restricciones, apareció una segunda posición dentro de la doctrina penal, postulando que los delitos informáticos son, en realidad, **conductas completamente nuevas**, que requieren de una regulación distinta y para las cuales no alcanza con los tipos penales tradicionales.

Finalmente, existe una tercera posición, adoptada por la legislación argentina y la que

EL PRECEDENTE LANATA EN LA ARGENTINA

En 1999, ante la inexistencia de una previsión expresa en el Código Penal, se discutió si el correo electrónico era asimilable al correo epistolar para fines penales. En el precedente Lanata, la justicia argentina determinó que sí lo eran.

Figura 7. **Es difícil conceptualizar si un delito informático es un delito común a través de medios informáticos o una conducta nueva.**

consideramos más adecuada, según la cual los delitos informáticos constituyen una categoría especial conformada por **delitos tradicionales cometidos por medios informáticos** y, asimismo, por **nuevas conductas nacidas en virtud del avance tecnológico**. Esta posición, que de algún modo permite compatibilizar las dos anteriores, parece la más razonable porque, efectivamente, hay ciertos delitos tradicionales que pueden cometerse aprovechando el uso y las potencialidades de las nuevas tecnologías (por ejemplo, los delitos vinculados a las calumnias o injurias, que vulneran el honor de las personas), pero también existen conductas cuyo encuadre en los tipos penales tradicionales es prácticamente imposible (por ejemplo, la figura del intrusismo informático o hacking).

Siguiendo esta posición, a continuación nos referiremos, en particular, a los delitos informáticos más comunes, pero aclaramos que no todos los países han reconocido estas figuras como delitos penales todavía.

LA VIOLACIÓN DEL CORREO ELECTRÓNICO Y DE LAS COMUNICACIONES POR INTERNET

El primer delito informático al que haremos referencia es la **violación del correo electrónico y de las comunicaciones por Internet**. En este sentido, debemos destacar que casi todas las constituciones modernas prevén específicamente la inviolabilidad de las comunicaciones y de los papeles privados. Luego, fundados en esas cláusulas constitucionales, los distintos códigos penales establecieron los delitos vinculados a la **violación de correspondencia** y la **violación de secretos**, en general.

Por lo tanto, este es un típico ejemplo de un delito penal que ya existía, y que debe ser actualizado con las nuevas formas de comisión que involucran a la tecnología.

Las acciones típicas que configuran este delito consisten en el **acceso**, **apoderamiento**, **captación** o **desvío**, o la **interceptación** de correos electrónicos u otro tipo de comunicaciones. En esta última categoría entrarían, por ejemplo, las comunicaciones privadas que puedan mantenerse a través de redes de mensajería instantánea (tipo Whatsapp), redes sociales (como Facebook) o redes de microblogging (como Twitter).

Habitualmente, se prevé como agravante, o bien como otro delito autónomo, la conducta

Figura 8. **La violación del correo electrónico fue uno de los primeros delitos informáticos denunciados ante las autoridades.**

de publicar estas comunicaciones privadas. Es decir, si además de acceder al contenido de los correos electrónicos de terceros en forma ilegítima, dichos contenidos son publicados o dados a conocer al público en general, estaríamos ante un delito más grave (agravado) o bien ante la comisión de otro delito, adicional al de violación de las comunicaciones. Esto depende de la legislación de cada país.

Es importante destacar que este delito informático se complementa con las normas que, en cada país, regulan los servicios de telecomunicaciones y prevén, en términos generales, la **inviolabilidad de las comunicaciones telefónicas**.

Por otra parte, debemos señalar que se trata de un delito que, habitualmente, solo admite la figura **dolosa**. Esto significa que solo puede cometerse si el autor lo hace con intención, excluyéndose la posibilidad de que se cometa por impericia, imprudencia o negligencia. Esto último es muy importante porque, si no fuera así, quien por un descuido accediera a un correo electrónico de otra persona (por ejemplo, porque la otra persona hubiera dejado su sesión iniciada en la computadora), estaría cometiendo un delito penal.

EL INTRUSISMO INFORMÁTICO O HACKING

El segundo delito informático al que haremos referencia es el denominado **intrusismo informático** o **hacking**. En este caso, nos encontramos ante una conducta nueva, que surge a partir del avance de las tecnologías de la información (y, por lo tanto, no estaba prevista en la normativa existente con anterioridad).

Habitualmente, la acción típica consiste en **acceder** a un sistema o dato informático **sin autorización** o **excediendo la autorización** que se posee. En principio, el delito se consuma con el acceso, por lo que no requiere que,

LA REGULACIÓN EN LA ARGENTINA

En la Argentina, la protección de las comunicaciones está prevista en la Constitución Nacional (art. 18), en el Código Penal (arts. 153 y 155), en la Ley de Telecomunicaciones (art. 18) y en La Ley de Inteligencia Nacional (art. 5).

Figura 9. **El hacking fue tal vez el primer delito informático que consistió en una conducta nueva.**

además, se provoque algún daño en los sistemas, se borre información, etcétera. En todo caso, esas acciones (daños, borrado de información, etc.) constituirán otros delitos, independientes de este.

Desde el punto de vista de la **autoría**, el delito puede ser cometido tanto por un tercero que no tenga relación con el titular del sistema informático, como por alguien que tenga relación (por ejemplo, un empleado), en cuyo caso podríamos estar ante un exceso en la autorización. Es decir, el empleado sabe que puede acceder hasta cierta parte del sistema o con ciertas finalidades, y excede sus autorizaciones.

Al igual que en el caso anterior, se trata de un delito **doloso**. Quien lo comete debe tener pleno conocimiento de que está accediendo a un sector o a información para la cual no tiene acceso. El hecho de que se exija el dolo es muy importante, porque protege a quienes, tal vez por error, pudieran haber accedido a un dato informático restringido.

EL DAÑO INFORMÁTICO

El **daño** es un delito contra la propiedad, que tradicionalmente se define como la destrucción, inutilización o alteración en general de una cosa mueble o inmueble o un animal, total o parcialmente ajeno.

LA REGULACIÓN DEL HACKING EN LA ARGENTINA

En la Argentina, el hacking está previsto como una figura residual, que solo se aplicará si no existe un delito más grave. Es decir, si además del acceso ilegítimo, se comete un daño, la figura que se aplicará es la de daño, y no, la de acceso ilegítimo.

En este caso, al igual que en el caso de **violación de las comunicaciones privadas**, nos encontramos ante una figura penal que ya existía y que debe ser actualizada para su aplicación al ámbito informático.

Es conveniene que el daño informático sea regulado en forma expresa en el Código Penal

En efecto, en la Argentina existieron diversos casos jurisprudenciales en los cuales se discutía si la figura tradicional del delito de daños podía ser aplicada, sin más, al ámbito informático. Y los resultados fueron completamente disímiles. Así, en el célebre caso del hacking a la Corte Suprema de Justicia de la Nación, por ejemplo, se sostuvo que no era posible dañar una página de Internet dado que no encuadraba en el concepto de cosa mueble o inmueble. Y por aplicación de los principios de prohibición de interpretación extensiva y analógica en materia penal, se consideró que no había delito penal alguno. Pero, por otra parte, en otro caso se consideró que el hecho de introducir un virus en un sistema informático podría ser considerado daño desde el punto de vista penal.

En cualquier caso, entendemos que resulta conveniente que el daño informático sea regulado en forma expresa en el Código Penal, para evitar pronunciamientos judiciales contradictorios como los mencionados en el párrafo precedente.

Así se hizo en la Argentina, ya que el tipo penal referido al delito tradicional de daños fue modificado por la Ley de Delitos Informáticos a fin de reconocer en forma expresa las acciones que constituyen **daño informático**.

En este contexto, en la actualidad se considera que las acciones típicas que configuran el daño informático son **destruir** o **inutilizar** datos, documentos, programas o sistemas informáticos. Asimismo, entran dentro del concepto de daño informático las actividades de **venta** y **distribución** de cualquier programa destinado a causar daños (por ejemplo, un virus).

También en este caso nos encontramos ante un delito que solo admite la comisión **dolosa**. Y, al igual que en los casos anteriores, resulta fundamental que este delito no admita la figura culposa, porque esto generaría un estado de inseguridad jurídica para las personas. En efecto, en la actualidad es muy común que ciertos programas maliciosos tomen control de la casilla de correo electrónico del usuario y, a través del envío de correos electrónicos masivos, se autodistribuyan. Si este delito admitiera la figura culposa, esos usuarios que, habiendo sido infectados, luego distribuyeran el virus, estarían cometiendo el delito.

LA ESTAFA INFORMÁTICA

La **estafa** es uno de los delitos penales más complejos y graves en el contexto de los delitos que afectan el patrimonio. Tradicionalmente, requiere para su consumación de un **engaño inicial** que determina que la víctima realice una **disposición**

Figura 10. **En un principio se discutía si podía existir daño informático, dado que la concepción tradicional implica romper algo físico.**

patrimonial en favor de quien comete el delito. Un ejemplo muy simple de este delito podría ser el de quien simula ser un cobrador de las cuotas de los asociados a un club. En este caso, el **engaño** consiste en que la persona simula tener una calidad que no tiene –la de cobrador del club– y, en virtud de eso, consigue que las víctimas, los asociados, le entreguen dinero (esta es la disposición patrimonial).

Ahora bien, en el delito tradicional de estafa, uno de los presupuestos era que existiera **contacto efectivo** entre la víctima y el autor del delito. Durante ese contacto efectivo es cuando se producía el engaño, que llevaba a la disposición patrimonial.

Esta situación cambió radicalmente con la introducción de las nuevas tecnologías, y generó situaciones que resultaban difíciles de encasillar en los moldes tradicionales de la estafa. Un caso típico de esto fue el de la **extracción ilegítima de dinero en cajeros automáticos** mediante el uso de tarjetas de débito duplicadas.

EL CASO NAPSTER

En este célebre caso, se consideró que dicho sitio había sido creado con la finalidad de vulnerar derechos de propiedad intelectual de terceros (concretamente, obras musicales). Por eso, el sitio debió dejar de operar del modo en que lo hacía.

Figura 11. **Las estafas en los cajeros automáticos pusieron en crisis el concepto clásico de estafa.**

En un importante caso que llegó a los tribunales argentinos se descubrió que la maniobra con la que se cometía el hecho implicaba el uso de diversos dispositivos tecnológicos que permitían copiar la información de la tarjeta de débito y, a su vez, obtener la clave (PIN) del usuario para generar tarjetas duplicadas y, con ellas, extraer dinero.

La operatoria era la siguiente:

1) En la entrada al cajero automático, se colocaba un dispositivo que, al pasar la tarjeta de débito para poder ingresar al recinto, copiaba la información de su banda magnética sin que el usuario lo percibiera.

2) Luego, en el propio cajero automático, se colocaba un dispositivo encima del teclado, que registraba la clave (PIN) del usuario también sin que este pudiera detectarlo.

3) Al final de cada día, los autores de esta compleja maniobra retiraban ambos dispositivos y, con eso, tenían toda la información necesaria para generar tarjetas de débito idénticas a las de los usuarios, con las cuales realizar extracciones de dinero.

Como puede apreciarse, los hechos descriptos implican que existe un engaño y, también, una disposición patrimonial, aunque no del modo previsto tradicionalmente en el delito de estafa. Esto es así porque, en primer término, la víctima del engaño sería el banco, que es quien –en el convencimiento de que la persona que está operando es el titular de la cuenta– entrega los fondos. Ahora bien, el banco, a su vez, no está representado por una persona sino por un cajero automático, que no es susceptible de ser engañado, porque no tiene voluntad, no es una persona. Y por otra parte, la disposición patrimonial no la realiza la víctima, como correspondería en el delito tradicional de estafa.

Todas estas complicaciones generaron un gran debate en los tribunales, y si bien en el caso que mencionamos se dijo que el delito cometido era el de **estafa**, no había unanimidad en tal apreciación.

En virtud de lo anterior, la Ley de Delitos Informáticos también modificó en la Argentina el delito de estafa, agregando el supuesto de **estafa informática**, que consiste en engañar a otro a través de la manipulación de un sistema informático o de transmisión de datos. En esta categoría están comprendidas, entre otras, las maniobras

de phishing, mediante las cuales se obtiene información acerca de cuentas bancarias para, luego, realizar transacciones fraudulentas.

LA DESTRUCCIÓN O ALTERACIÓN DE PRUEBA INFORMÁTICA

Uno de los problemas más frecuentes en el ámbito de los delitos informáticos es el relativo a la prueba de tales conductas. En este sentido, como vimos al explicar los principios que se aplican en el Derecho Penal, la prueba de un delito debe ser concluyente, porque debe destruir la **presunción de inocencia** de la persona imputada. Es por eso que quien comete un delito muchas veces procura borrar sus huellas destruyendo información o documentación que podrían incriminarlo.

Es para este supuesto que en algunas legislaciones existe una figura penal autónoma, relativa a la destrucción de prueba informática. Un delito que es independiente del delito que se quisiera ocultar mediante esta destrucción de prueba.

En la Argentina, la Ley de Delitos Informáticos reguló este delito indicando que la acción típica consiste en **sustraer, alterar, ocultar, destruir** o **inutilizar** elementos que pudieran servir como prueba en un proceso judicial. Dentro de este concepto estarían comprendidos los registros informáticos.

Es importante destacar que este delito es el único de los delitos informáticos que no solo admite la comisión **dolosa**, sino que también se puede cometer por negligencia, impericia o imprudencia (figura **culposa**). En efecto, este tema no es menor, porque podría desencadenar la responsabilidad penal del administrador de la red si este borrase elementos que pudieran servir como prueba en un proceso judicial.

Ahora bien, ¿cómo debería actuar el administrador de la red para evitar la comisión de este delito en su forma culposa? La responsabilidad del administrador respecto de esta figura penal requiere que él conozca la existencia de un proceso judicial en el cual la información que administra pueda servir como prueba. Por lo tanto, desde el momento en que el administrador es notificado de la existencia de un proceso judicial que involucra a usuarios de su red o a la empresa en la que trabaja, debería extremar los recaudos para evitar eliminar información que pudiera ser útil a los fines de ese proceso (por ejemplo, logs y otra información que surja de la red).

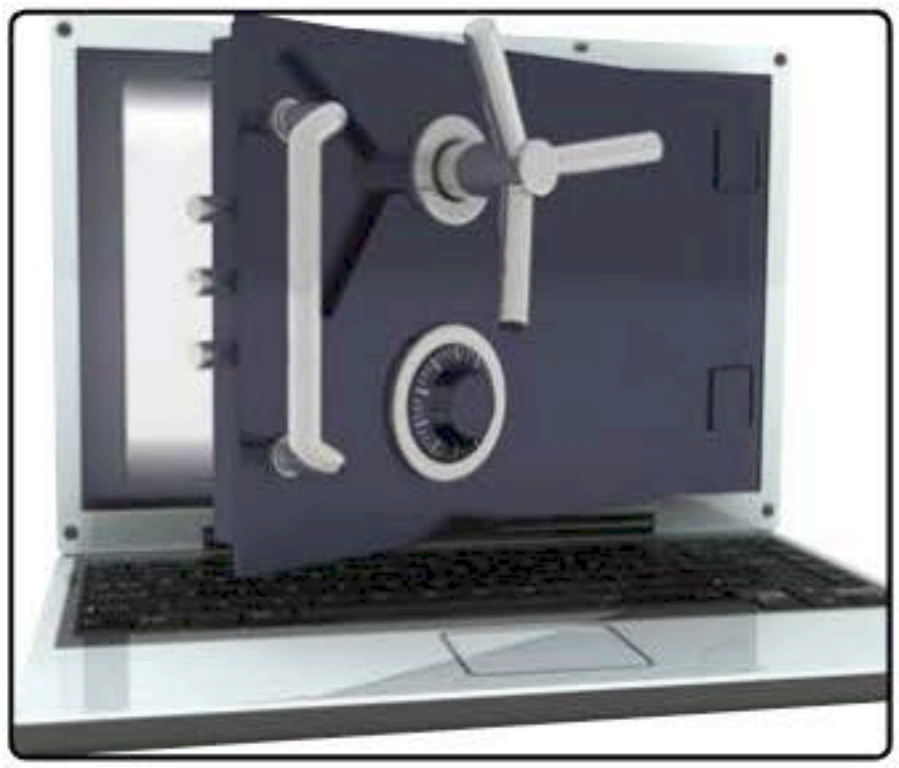


Figura 12. **Destruir u ocultar evidencia electrónica es un delito autónomo, que puede cometerse aun en forma culposa.**

Por otra parte, a fin de evitar cuestionamientos respecto de sus decisiones al manipular la información que podría servir de prueba en procesos judiciales, resulta conveniente que en la organización exista un protocolo de actuación respecto de la recolección y almacenamiento de información. De este modo, la responsabilidad personal del administrador de la red se vería reducida, porque él no tomaría la decisión respecto de cuándo eliminar información o qué información guardar, sino que esto provendría del protocolo, que el administrador debe cumplir.

DELITOS VINCULADOS A LA VIOLACIÓN DE DERECHOS DE PROPIEDAD INTELECTUAL

Por último, haremos referencia a ciertos delitos que podrían ser cometidos por los usuarios de la red, pero que, en algunos casos, podrían comprometer la responsabilidad tanto civil como penal de su administrador.

Nos estamos refiriendo, puntualmente, a los delitos vinculados a la **violación de derechos de propiedad intelectual**. Estos consisten en diversas acciones que tienen como finalidad **copiar**, **alterar** y/o **distribuir** –con o sin ánimo de lucro– obras protegidas por derechos de propiedad intelectual sin autorización de sus autores.

Dentro del concepto de obra están comprendidas las canciones, películas, imágenes, guiones, libros, software (tanto el código fuente como el objeto) y cualquier otra obra que tenga protección bajo derechos de propiedad intelectual.

Figura 13. **En el caso Napster se juzgó a los dueños de la plataforma de intercambio de archivos.**

Los delitos vinculados a la violación de derechos de propiedad intelectual son, sin dudas, los que más crecieron con el desarrollo de las tecnologías de la información. Es que la interconexión en las redes permitió que las personas comenzaran a **compartir** distintas obras, sin autorización o excediendo la autorización de los titulares de los derechos de propiedad intelectual.

En el ámbito internacional, tal vez los casos más paradigmáticos en los que se persiguió este tipo de acciones fueron los casos de **Napster** y, luego, **Groekster**, ambos tramitados en los Estados Unidos. Más recientemente, también tuvo mucha trascendencia el caso **MegaUpload**, aunque el momento de escribir este libro, aún no tiene sentencia definitiva. En todos ellos se persiguió a quienes cometían y/o instigaban a cometer delitos contra la propiedad intelectual mediante la distribución de obras de diverso tipo sin autorización de sus autores.

Todos estos delitos vinculados a la propiedad intelectual son **delitos dolosos**, que requieren de la intención del autor para configurarse. Entonces, ¿por qué podría responsabilizarse al administrador de una red por los delitos contra

la propiedad intelectual que pudieran cometer los usuarios de dicha red?

En la Argentina existen dos casos, que se están tramitando en la actualidad (por lo que no tenemos certeza acerca de cómo serán resueltos), que se basan en un criterio que, de confirmarse, podría determinar que los administradores de redes sean imputados penalmente en determinadas circunstancias.

El primer caso es el denominado caso **Taringa!**, en el cual se está juzgando la eventual responsabilidad de los titulares de un famoso sitio de Internet –que, a su vez, serían titulares de la empresa que provee el hosting a dicho sitio– por la violación a derechos de propiedad intelectual que habrían realizado los usuarios. El fundamento para responsabilizar penalmente a los titulares del sitio sería que, si bien no son los autores de los delitos, son partícipes necesarios en ellos. En otras palabras, lo que se estaría proponiendo es que, si el sitio web en cuestión no existiera, no se cometerían esos delitos (y, por lo tanto, si los delitos se cometen, existe una responsabilidad también de los titulares del sitio, aunque no sea directa).

El segundo caso es aún más complicado desde el punto de vista de la responsabilidad penal. Se trata del caso en el que se juzga la eventual responsabilidad del titular de un sitio de streaming denominado **Cuevana**, también muy famoso. Este sitio presenta links a otros sitios que tienen contenido audiovisual, de modo tal de facilitar que dicho contenido sea accesible a los usuarios con una interfaz muy amigable. En principio, el sitio no almacenaría el contenido sino que solo proveería la plataforma tecnológica que permitiría reproducir los contenidos desde los sitios en los que están almacenados. Sería como una suerte de "puente" entre dichos contenidos y los usuarios. Así las cosas, existe una denuncia penal presentada por un fiscal contra el titular del sitio, señalándolo como coautor de delitos contra la propiedad intelectual, debido a que gran parte del contenido audiovisual al que puede accederse a través del sitio es contenido ilegítimo (porque no ha sido autorizado por sus autores).

En ambos casos, se aplica un criterio de responsabilidad para quienes administran o dirigen sitios de Internet o empresas de hosting, que podría aplicarse también a los administradores de una red. Según este criterio, el administrador

Figura 14. **El streaming de video está generando discusiones sobre la responsabilidad penal de quienes diseñan los sitios de acceso.**

de la red podría ser partícipe necesario –caso Taringa!– o coautor –caso Cuevana– de los delitos contra la propiedad intelectual que pudieran cometer los usuarios de la red.

Entonces, ¿qué debería hacer el administrador de la red para evitar ser responsabilizado por la actividad de los usuarios? De acuerdo con lo que surge de los pronunciamientos judiciales dictados en distintos lugares del mundo con relación a este tema, podemos formular una serie de reglas generales que deberían cumplirse para limitar al máximo la responsabilidad del administrador de la red por las acciones de los usuarios. Estas reglas son:

1) Procurar que existan políticas de uso en la red que contengan cláusulas específicas referidas a la obligación de los usuarios de no distribuir a través de la red contenidos protegidos por derechos de propiedad intelectual sin autorización de sus titulares, ni utilizar la red para bajar dichos contenidos.

2) Generar mecanismos automáticos que, sin violar la privacidad de las comunicaciones de los usuarios, permitan controlar el cumplimiento de estas políticas de uso (porque una de las cuestiones que habitualmente se critica en los pronunciamientos judiciales es que las políticas existen, pero no se hacen cumplir).

3) Adoptar un mecanismo sencillo y rápido que permita que los titulares de derechos de propiedad intelectual que pudieran verse afectados por algún usuario de la red lo denuncien fácilmente, de modo tal que sus contenidos puedan ser eliminados de la red.

4) En caso de detectar violaciones a derechos de propiedad intelectual en forma sistemática por parte de algún usuario, debería analizarse la posibilidad de aplicar alguna sanción a dicho usuario, que podría incluir la limitación de su actividad en la Red.

RESUMEN

Los delitos informáticos desafían al sistema penal porque las reglas de interpretación de la ley penal colisionan con las nuevas conductas o medios comisivos. Es por eso que resulta conveniente el dictado de una ley especial que contemple estas figuras.

Capítulo 4

Recursos informáticos en el ámbito laboral

Veremos las tecnologías de la información en el trabajo, la posibilidad de monitorear su uso y los límites al control.

RedUSERS.com

El control del uso **de recursos informáticos en el ámbito laboral**

En este capítulo analizaremos la problemática que ha generado la informática en el ámbito del trabajo, con especial referencia a aquellas cuestiones que podrían resultar de interés para el administrador de una red corporativa.

Con tal fin, mencionaremos en primer término algunos principios y criterios de interpretación propios del **Derecho del Trabajo**, que es la disciplina jurídica encargada de regular la relación entre los trabajadores y sus empleadores. Luego, repasaremos las situaciones problemáticas que suelen darse en el ámbito laboral como consecuencia de la utilización de los recursos informáticos como herramientas de trabajo.

Figura 1. **En el contrato de trabajo las partes no están en igualdad de condiciones.**

Ámbito de aplicación **del Derecho del Trabajo**

Como adelantamos, el **Derecho del Trabajo** se ocupa de regular la relación existente entre trabajadores y empleadores.

En el ámbito privado, la relación laboral se basa en un **contrato de trabajo**, que es un acuerdo de voluntades con la particularidad de que una de las partes, el empleador, tiene habitualmente una posición sustancialmente más fuerte que la otra, el trabajador.

Teniendo en cuenta esta disparidad de fuerzas, el Derecho del Trabajo procura equiparar de algún modo la situación del trabajador, para evitar que el empleador pueda cometer abusos derivados de su posición.

Es por eso que la interpretación del **contrato de trabajo** es diferente de la interpretación de cualquier otro contrato, en el que las partes son libres de negociar los términos de contratación. En el caso del contrato de trabajo, como veremos a continuación, **lo que las partes pacten**

solo será válido en la medida en que cumpla con los principios y reglas del Derecho del Trabajo. En caso contrario, dichas convenciones podrán ser anuladas judicialmente.

En virtud de lo expuesto, si se considera al contrato de trabajo como el conjunto de normas que regulan la relación entre el trabajador y su empleador, podemos concluir en que dicho conjunto está conformado por:

1. El **contrato individual**, que es el que el trabajador firma con el empleador.

2. Las **disposiciones legales** que regulan la relación laboral (por ejemplo, en la Argentina, la Ley de Contrato de Trabajo N° 20.744 y sus normas complementarias).

3. Las disposiciones convencionales, que surgen del **Convenio Colectivo de Trabajo** que resulte aplicable a la relación.

Como veremos más adelante, en virtud del denominado **orden público laboral**, el contrato individual no podría nunca establecer condiciones que, respecto de los derechos del trabajador, estén por debajo de las establecidas en la ley y en el Convenio Colectivo de Trabajo aplicables a la relación.

Figura 2. Los trabajadores conforman sindicatos que, luego, negocian Convenios Colectivos de Trabajo.

Es importante aclarar que los principios que veremos a continuación resultan aplicables, con algunas variantes, en gran parte de los países con derecho de fuente continental europea (es decir, los que no aplican el **Common Law**), aunque las referencias normativas que mencionaremos serán, predominantemente, de leyes argentinas.

EL TRABAJO EN EL ÁMBITO PÚBLICO

Los principios que mencionamos en este capítulo son aplicables al trabajo en el ámbito privado. En el ámbito público, las normas que rigen el trabajo son normas de derecho administrativo, ya que se considera que el empleado es un agente estatal.

EL PRINCIPIO DE LA REALIDAD POR SOBRE LAS FORMAS

El **principio de la realidad por sobre las formas** determina que, más allá de la calificación que las partes pudieran dar a su relación, será el juez quien la defina atendiendo a la realidad de los hechos.

Esto quiere decir que aunque las partes firmen un documento indicando que son contratistas independientes y que, por lo tanto, su relación no es de índole laboral, dicho documento será considerado nulo si un juez determina que, en la realidad, la relación era de índole laboral.

En principio, se considerará que hay **relación laboral** cuando estén presentes las tres notas típicas de esta relación:

1. La subordinación económica.
2. La subordinación jurídica.
3. La subordinación técnica.

En la tabla de la siguiente página nos referiremos a cada una de ellas con mayor detalle.

EL PRINCIPIO IN DUBIO PRO TRABAJADOR

Este principio funciona de un modo similar al principio **in dubio, pro reo**, que vimos en el Capítulo 3 de este libro. Su aplicación tiene lugar en los procesos judiciales, y determina que, en caso de dudas, el juez debe decidir la cuestión a favor del trabajador.

En cuanto a su alcance, en algunas legislaciones se refiere **únicamente a dudas sobre el derecho aplicable**, mientras que en otras legislaciones de aplica también a **dudas sobre la prueba** producida en la causa.

EL ORDEN PÚBLICO LABORAL Y EL PRINCIPIO DE IRRENUNCIABILIDAD

Dentro del sistema jurídico existen normas que han sido concebidas para regir situaciones en que las partes no hayan pactado nada en forma expresa, pero que pueden ser dejadas de lado por ellas. Estas normas se denominan **normas suplementarias** o **dispositivas**.

Por ejemplo, en los países que poseen leyes civiles, el contrato de compraventa suele estar regulado expresamente, lo que permitiría a las partes omitir ciertos términos del contrato

CONVENIOS COLECTIVOS DE TRABAJO

Son acuerdos que firman las cámaras empresariales (en representación de los empleadores) con los sindicatos (en representación de los trabajadores), y obligatorios para todos los trabajadores y empleadores comprendidos en su ámbito de aplicación.

NOTAS TÍPICAS DE LA RELACIÓN LABORAL	
Subordinación económica	El trabajador depende para su subsistencia del salario que, por su trabajo, le paga el empleador.
Subordinación jurídica	El empleador tiene la potestad de dirigir los objetivos del trabajo a fin de alinearlos a los de la empresa. Puede dar órdenes, dentro del marco de atribuciones que la ley le confiere, y eventualmente, también puede ejercer las facultades disciplinarias respecto del trabajador.
Subordinación técnica	El trabajador debe realizar las tareas de acuerdo con los lineamientos técnicos que le indique el empleador. Esta nota tipificante suele estar atenuada en los casos de trabajadores profesionales o técnicos con alta especialización, porque en esos casos, el empleador suele no tener tantos conocimientos como para dirigir técnicamente al trabajador.

Tabla 1. **Las notas típicas de la relación laboral la distinguen de otros tipos de relaciones jurídicas.**

porque estos surgen de las normas que lo regulan. Ahora bien, si las partes deciden acordar términos específicos, podrían hacerlo aun en contra de lo que dice la legislación.

Sin embargo, existen algunas normas que nunca pueden ser dejadas de lado por las partes, estas son las **normas imperativas**. Las normas imperativas conforman lo que se conoce como **orden público**. Por lo tanto, cuando en el ámbito jurídico se menciona el concepto de orden público, se está haciendo referencia a normas que no pueden ser dejadas de lado por las partes.

¿CONTRATO DE TRABAJO SIN CONTRATO?

En las legislaciones de diferentes países (por ejemplo, en la Argentina), el contrato de trabajo no está sujeto a ningún requisito de formalidad. Por lo tanto, puede ocurrir que no exista un contrato de trabajo escrito.

En este contexto, podemos decir que el **orden público laboral** está conformado por el conjunto de derechos que las normas laborales confieren al trabajador. Se trata de un orden público particular, porque **puede ser dejado de lado por las partes siempre que sea para beneficio del trabajador**. Por eso se dice que las normas laborales establecen un piso para los derechos de los trabajadores.

Estrechamente vinculado al orden público laboral se encuentra el **principio de irrenunciabilidad**, que determina que –como regla general– el trabajador no pueda renunciar a sus derechos.

Figura 3. **El trabajador no puede renunciar a sus derechos. Si lo hace, la renuncia será nula.**

El alcance del principio de irrenunciabilidad podría variar según las legislaciones. En las más protectorias, el trabajador no podría renunciar a ningún derecho; mientras que en las más flexibles, podría renunciar a los derechos del contrato individual siempre que sean superiores a los establecidos en la ley y el Convenio Colectivo de Trabajo aplicable.

¿POR QUÉ ES IMPORTANTE CONOCER LOS PRINCIPIOS DEL DERECHO DEL TRABAJO?

Alguien podría preguntarse por qué repasamos algunos principios generales del Derecho del Trabajo en una obra dedicada a administradores de redes.

La explicación es sencilla: dado que, en términos generales, no hay legislación específica referida a la utilización de medios informáticos en el ámbito laboral, los problemas que surgen deben ser resueltos aplicando los principios generales del Derecho del Trabajo y adecuando las normas existentes al caso particular.

En este contexto, la situación del administrador de una red corporativa suele ser bastante complicada: para algunas situaciones, tendrá una clara

EL PRINCIPIO IN DUBIO, PRO TRABAJADOR

En la Argentina, a partir del año 2008 se adoptó de manera expresa en la Ley de Contrato de Trabajo el criterio amplio del in dubio, pro trabajador, aplicándolo también a la prueba.

posición de **trabajador** de la empresa propietaria de la red, pero, a su vez, ejercerá ciertas potestades respecto de los usuarios de dicha red –que también podrían ser trabajadores–, que lo acercarán más al concepto de **empleador**.

Es por eso que resulta fundamental conocer los principios mencionados en este capítulo para, con ellos, poder resolver los problemas que, en el día a día, puedan plantearse.

El empleador y el **control del uso de los recursos informáticos**

El principal problema surgido con motivo del uso de recursos informáticos en el ámbito laboral es la tensión existente entre la **facultad de control** que tiene el empleador y el **derecho a la intimidad** del trabajador. Es que los recursos informáticos proporcionan una mayor posibilidad de control de los trabajadores por parte del empleador, que si se ejerce abusivamente, podría resultar violatorio de su intimidad.

A modo de ejemplo de lo que desarrollaremos más adelante, podemos mencionar la posibilidad de que el empleador monitoree dónde se encuentran los trabajadores en todo momento mediante el uso de tecnologías de GPS en los teléfonos celulares provistos por la empresa. Este tipo de control, si se ejerce en horario no laboral, sería claramente abusivo (el empleador no tiene derechos ni facultades para conocer dónde están los trabajadores fuera del horario de trabajo, dado que esto es parte de su vida privada).

Figura 4. **El empleador puede monitorear el uso de los recursos informáticos, pero respetando los derechos de los trabajadores.**

EL PRINCIPIO DE IRRENUNCIABILIDAD EN LA ARGENTINA

Desde el año 2009, la Argentina adoptó expresamente el criterio más protectorio del principio de irrenunciabilidad en la Ley de Contrato de Trabajo, disponiendo que son irrenunciables todos los derechos laborales.

A continuación, nos referiremos a distintos supuestos en que esta **tensión de derechos** suscitó conflictos que tuvieron que ser resueltos por la justicia.

EL MONITOREO DEL CORREO ELECTRÓNICO LABORAL

Por una cuestión temporal, el primer conflicto que se planteó estuvo relacionado con el monitoreo del correo electrónico laboral por parte del empleador.

Ante todo, debemos aclarar que nos estamos refiriendo al correo electrónico que, en el marco de una relación laboral, el empleador otorga al trabajador para que este pueda realizar más eficientemente sus tareas. No nos referimos al **correo electrónico privado** del trabajador, que **nunca podrá ser monitoreado por el empleador**, dado que esto no solo sería un ilícito para el Derecho Laboral sino que, como vimos en el Capítulo 3, también constituiría un **delito penal**.

En este contexto, los primeros conflictos judiciales surgieron con motivo de despidos realizados en virtud del uso del correo electrónico laboral para fines personales. En estos primeros casos,

Figura 5. **Que el correo electrónico laboral requiera una clave puede generar una expectativa de privacidad en los trabajadores.**

los trabajadores argumentaban que los despidos eran injustos, entre otras cosas, porque el empleador no había advertido que el uso del correo electrónico estaría monitoreado y, por lo tanto, se había generado una expectativa de privacidad en los trabajadores.

En una primera etapa, los tribunales en general hicieron lugar a los pedidos de los trabajadores y consideraron ilegítimos los despidos teniendo especialmente en cuenta la **inexistencia de políticas de uso de los recursos**

LA DIRECCIÓN DE CORREO ELECTRÓNICO LABORAL

La dirección de correo electrónico laboral suele estar conformada por el nombre del trabajador, seguido del signo arroba (@) y, luego, el dominio de Internet del empleador, que habitualmente coincide con su marca o denominación social.

informáticos. Esta circunstancia se sumaba al hecho de que no se había advertido a los trabajadores acerca del monitoreo del uso de los recursos informáticos.

Con relación a las políticas de uso de los recursos informáticos, en algunos pronunciamientos se mencionó que debía acreditarse su correcta notificación a los trabajadores, y que, además, debían ser razonables. Esta **razonabilidad** exigida por los jueces se refiere, fundamentalmente, a la **adecuación entre las infracciones y las sanciones** previstas en dichas políticas.

En algunos casos más recientes, también se exigió la prueba de que las políticas de uso de los recursos informáticos se cumplen efectivamente en la empresa, y que no se han redactado al solo fin de cumplir con una obligación formal. En este sentido, también se sostuvo que las políticas **deben aplicarse a todos los trabajadores por igual**, dado que, en caso contrario, se daría un supuesto de discriminación.

En definitiva, la justicia ha convalidado las facultades del empleador para monitorear el uso del correo electrónico laboral de los trabajadores, pero siempre que se cumplan ciertos requisitos. Entre ellos, además de los que mencionamos precedentemente, se exigió que las sanciones por incumplimiento de las políticas de uso de los recursos informáticos tengan los mismos recaudos que cualquier otra sanción laboral.

EL MONITOREO DEL USO DE LA CONEXIÓN A INTERNET

Respecto del uso de la conexión a Internet, no ha habido tanta conflictividad como respecto del uso del correo electrónico laboral.

Tal vez esto se deba a que, en el uso de la conexión a Internet, por su naturaleza, **no exista una tan clara expectativa de privacidad** como en el correo electrónico (en efecto, para el correo electrónico el trabajador generalmente tiene la posibilidad de establecer su propia clave de acceso, mientras que para el uso de Internet es menos frecuente que eso ocurra).

Ahora bien, si se plantease un conflicto judicial referido al monitoreo del uso de la conexión a Internet provista por el empleador, entendemos que, en principio, deberían aplicarse los criterios que reseñamos para el caso del correo electrónico laboral. Decimos en principio porque, al monitorear el uso de la conexión a Internet, podría

EL CASO DE LOS TELETRABAJADORES

En algunas legislaciones, se exige que el empleador reconozca a los teletrabajadores una parte o todo el costo del acceso a Internet. A pesar de esto, el empleador no podría ejercer ningún tipo de monitoreo en estos casos.

ocurrir que el empleador se encuentre con comunicaciones privadas del trabajador (por ejemplo, si el trabajador ingresara en su cuenta de correo electrónico personal utilizando la conexión a Internet de la empresa). En estos casos, si bien el monitoreo en sí sería legítimo, el empleador no

REQUISITOS PARA LA VALIDEZ DEL MONITOREO DEL CORREO ELECTRÓNICO LABORAL POR PARTE DEL EMPLEADOR	
Eliminación de la expectativa de privacidad del trabajador	El empleador debe comunicar al trabajador, de un modo claro y expreso, que el correo electrónico laboral será monitoreado.
Existencia de políticas de uso de los recursos informáticos	El empleador debe notificar a los trabajadores acerca de las políticas de uso de los recursos informáticos, que deben contener: las conductas esperadas, las conductas prohibidas y las sanciones en caso de incumplimiento, que deben ser razonables.
Aplicación de las políticas a todos los trabajadores por igual.	Las políticas de uso de los recursos informáticos deben ser aplicadas a todos los trabajadores por igual, y debe exigirse su cumplimiento.
Aplicación de los criterios generales en materia de sanciones	Si el empleador decidiera sancionar a algún trabajador por violación de las políticas de uso de los recursos informáticos, la sanción debería cumplir con los requisitos de validez aplicables a cualquier sanción laboral: 1. Deberá ser proporcional a la falta. 2. Deberá ser contemporánea a la falta. 3. Deberá aplicarse respetando el derecho de defensa del trabajador. 4. No deberá ser discriminatoria ni persecutoria. 5. En su graduación, deberán tenerse en cuenta los antecedentes y las condiciones personales del trabajador.

Tabla 2. Estos requisitos deben cumplirse para que el monitoreo del uso del correo electrónico laboral sea considerado válido.

podría continuar monitoreando al advertir que el trabajador ha ingresado en un ámbito en el que sus comunicaciones se encuentran protegidas. Es decir, lo que debería hacer el empleador en tal caso es dejar de monitorear, y eventualmente, podría sancionar al trabajador por el uso de Internet para fines personales.

Finalmente, debemos señalar que **el empleador puede limitar el uso de Internet**, restringiendo el acceso a ciertos sitios tanto mediante la **prohibición jurídica** (contenida en las políticas de uso) como mediante la aplicación de **medidas técnicas** que limiten el acceso.

Figura 6. **El empleador puede legítimamente restringir el acceso a ciertos sitios de Internet.**

EL MONITOREO DE LA UTILIZACIÓN DE REDES SOCIALES

En el último tiempo, la mayor fuente de conflictos vinculados al uso de tecnologías en el ámbito laboral tuvo en el centro de la escena a las **redes sociales**.

Lo que ocurre es que, a través de estas redes, se ha producido un fenómeno vinculado a la **absoluta falta de privacidad** por parte de los usuarios. El concepto que promueven muchas redes sociales es que lo interesante es **compartir**. Y muchas veces, en el afán de compartir más y más, se divulga información que las organizaciones desearían mantener confidencial.

Por otra parte, del análisis de las participaciones de una persona en redes sociales, se puede trazar un perfil bastante preciso sobre su personalidad, lo cual en ocasiones también resulta interesante para el empleador.

A continuación analizaremos, bajo la óptica de las normas y principios del Derecho del Trabajo, las distintas cuestiones que se han planteado respecto de las redes sociales.

CLAVES DE ACCESO A LAS REDES SOCIALES

El empleador no puede, en ninguna circunstancia, requerir al trabajador que le entregue sus credenciales de acceso a las redes sociales. Tal conducta atenta contra la buena fe que debe primar en el contrato de trabajo.

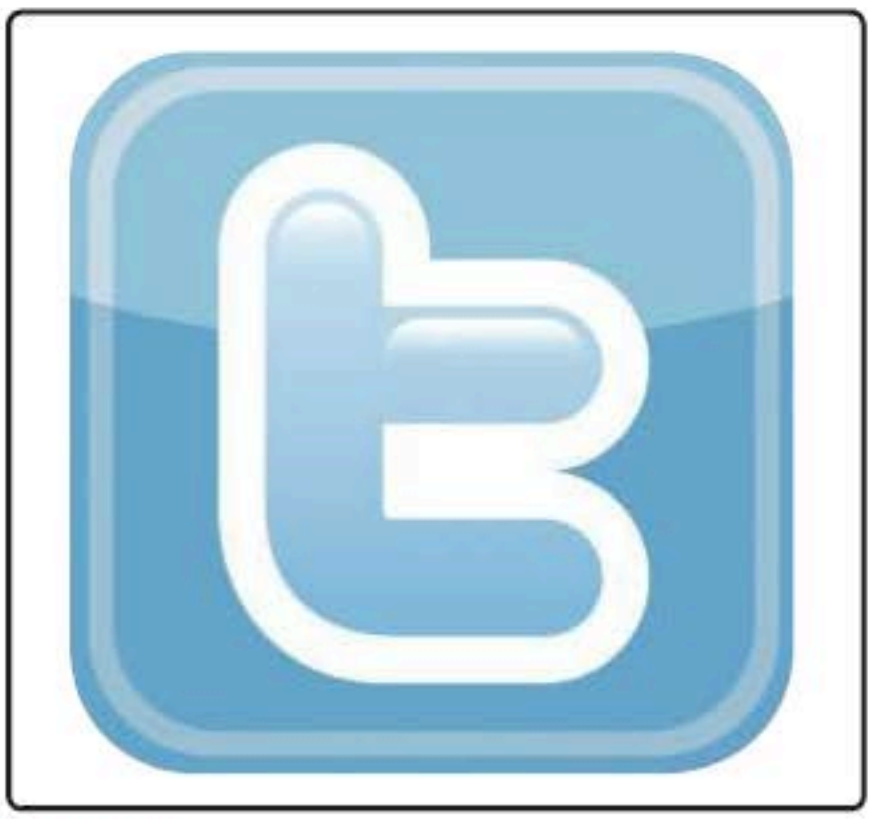


Figura 7. **Lo que publican los empleados en las redes sociales se refiere a la vida privada de los trabajadores.**

Monitoreo del uso de redes sociales en el trabajo

El primer supuesto que analizaremos es el del monitoreo de la utilización de las redes sociales por parte de los trabajadores en horario y lugar de trabajo.

En este caso, corresponde diferenciar si el trabajador está utilizando los medios informáticos provistos por el empleador para trabajar o si está usando medios informáticos propios (por ejemplo, un teléfono celular de su propiedad).

En el primer caso, es decir, si el trabajador está utilizando los medios informáticos provistos por el empleador para trabajar, entonces el monitoreo podría ser legítimo. No obstante, resultaría de aplicación lo que mencionamos respecto del monitoreo del acceso a Internet: el empleador no puede leer y espiar los contenidos que el trabajador publique en la red social, porque son parte de su vida privada. Lo que el empleador eventualmente podría hacer es sancionar al trabajador por violar las políticas de uso de los recursos informáticos, pero no podrá seguir **espiándolo**.

Si el trabajador accede a la red social desde sus propios medios informáticos, entonces el empleador no puede monitorear de modo alguno sus acciones. Desde ya que si el empleador advirtiese que el trabajador está teniendo actividad en redes sociales en horario de trabajo, podría sancionarlo disciplinariamente por no tener su fuerza de trabajo a disposición del empleador, pero no podría monitorear su actividad.

Cuando el trabajador autoriza al empleador a ver su actividad en las redes sociales

Existen algunos casos en los cuales el trabajador ha autorizado al empleador a ver su

DERECHO DE DEFENSA

Para sancionar a un trabajador por una falta, es necesario garantizar su derecho de defensa. El trabajador tiene derecho a presentar su descargo y a que dicho descargo sea tenido en cuenta antes de la aplicación de la sanción.

actividad en las redes sociales. Esta autorización consiste, por ejemplo, en **agregarlo como amigo** (en **Facebook** y redes similares) o permitir **que sea un seguidor** (en **Twitter** y redes similares).

En estos casos, si el trabajador autorizó **libremente** al empleador a ver su actividad, consideramos que no existe problema en que el empleador lo haga. Sin embargo, habrá que evaluar en cada caso si la autorización fue libre, dado que si se verificase que el trabajador autorizó al empleador por un requerimiento de este último, el consentimiento del trabajador podría estar viciado (por aplicación de los principios del Derecho del Trabajo, según los cuales el trabajador muchas veces no puede decir que no a un pedido del empleador).

Ahora bien, aun en caso de que el trabajador hubiera autorizado al empleador para que vea su actividad en las redes sociales, en principio este no tiene ninguna potestad respecto de tal actividad. Esta situación podría ser algo diferente si la empresa tuviera políticas específicas de uso de redes sociales.

Políticas de uso de redes sociales

Dadas las particulares características de las redes sociales, las empresas están comenzando a desarrollar **políticas específicas** para su uso.

Las políticas de uso de recursos informáticos en general resultaron insuficientes con relación a las redes sociales, dado el impacto social y cultural que tuvieron estas comunidades virtuales.

Figura 8. **Si el trabajador agrega libremente al empleador como amigo, el acceso del empleador es legítimo.**

Sin embargo, la redacción de este tipo de políticas es ciertamente difícil en el marco del Derecho del Trabajo, porque implica la confrontación entre dos derechos: **el de la empresa, a cuidar su imagen y su información**; y **el del trabajador, a tener una vida privada** sin injerencias externas.

Las políticas de uso de redes sociales suelen incorporar obligaciones que, en algunos casos, podrían considerarse abusivas, como que el trabajador no pueda publicar fotos personales en situaciones indecorosas. Esta obligación, por ejemplo, en el contexto de una política de uso de las redes sociales de una empresa que produce películas para niños, podría resultar razonable para dicha empresa. Pero, por otro lado, el trabajador afectado podría argumentar que él, fuera del trabajo, en su vida privada, tiene libertad para hacer lo que desee.

Figura 9. **Para evitar filtrado de información confidencial en redes sociales, las empresas desarrollan políticas específicas de uso.**

Lo que más complica la interpretación normativa en el caso de las redes sociales es que, por una parte, la actividad en dichas redes aparece como una **actividad privada**, que hace a la **intimidad** de las personas. Sin embargo, en muchos casos, la actividad dista de ser privada para ser una **actividad más bien pública**. Y esta distinción es fundamental para determinar cuándo una obligación exigida al trabajador es razonable. Si la actividad en redes sociales fuese privada, entonces la empresa no tiene injerencia alguna; pero si, por el contrario, se considerase que la actividad es **pública**, entonces la empresa podría tener algún interés jurídicamente relevante en establecer algunos parámetros para ella. Debemos señalar que, aun en este último supuesto, los parámetros deberían ser únicamente los necesarios para que la actividad del trabajador no afecte la imagen de la empresa, pero sin limitar la **libertad** del trabajador.

RESUMEN

El uso de la tecnología incrementa las posibilidades de control del empleador y, a la vez, puede afectar la intimidad de los trabajadores. Mediante la aplicación razonable de los principios del Derecho del Trabajo, debe procurarse un equilibrio.

Capítulo 5

La responsabilidad del administrador

Conoceremos los alcances y las formas de atenuar la responsabilidad civil del administrador de redes.

RedUSERS.com

La responsabilidad **del administrador de la red**

En este capítulo profundizaremos el análisis de la responsabilidad del administrador de una red. Tener **responsabilidad** significa que, en caso de se produzca algún daño, será él quien deba repararlo. Y si se tratase de un **delito**, entonces también podría ser el administrador quien, además de la eventual reparación civil, deba cumplir la condena correspondiente.

Como veremos, la particular situación en la que se encuentra el administrador de la red determina que su responsabilidad, en algunos casos, no se limite a sus propias acciones. En efecto, podría ser responsable por acciones de la empresa titular de la red que administra o, incluso, de los usuarios de dicha red.

Figura 1. **La responsabilidad civil es de contenido patrimonial. Su finalidad es resarcir a la víctima.**

Como explicamos en el Capítulo 1 de esta obra, la responsabilidad civil tiene como principal finalidad reparar un daño. El daño se repara, en primer término y si esto fuera posible, volviendo las cosas al estado anterior a que ocurriera la acción que causó el daño.

Ahora bien, si esto no fuera posible, entonces se procura resarcir a la víctima del daño, de modo de compensar de algún modo la lesión que ha sufrido en sus bienes o sentimientos.

Es decir, se trata de una **responsabilidad patrimonial**. Es por eso que en el ámbito de la responsabilidad civil no rigen las estrictas normas de interpretación que vimos en el Capítulo 3, por lo que son válidas las interpretaciones analógicas o extensivas, y actualmente, el Derecho Civil tiene un enfoque más basado en la **víctima** que en el hecho en sí.

En este contexto, ante todo, debemos establecer una distinción para el caso del administrador de la red que es **empleado**, respecto del que es un **contratista independiente**.

EL ADMINISTRADOR DE LA RED EMPLEADO

Respecto del administrador que es empleado de la empresa titular de la red, su responsabilidad civil frente a terceros se encuentra sustancialmente acotada.

En efecto, en términos generales, las legislaciones de los distintos países establecen que el empleador debe responder civilmente por las

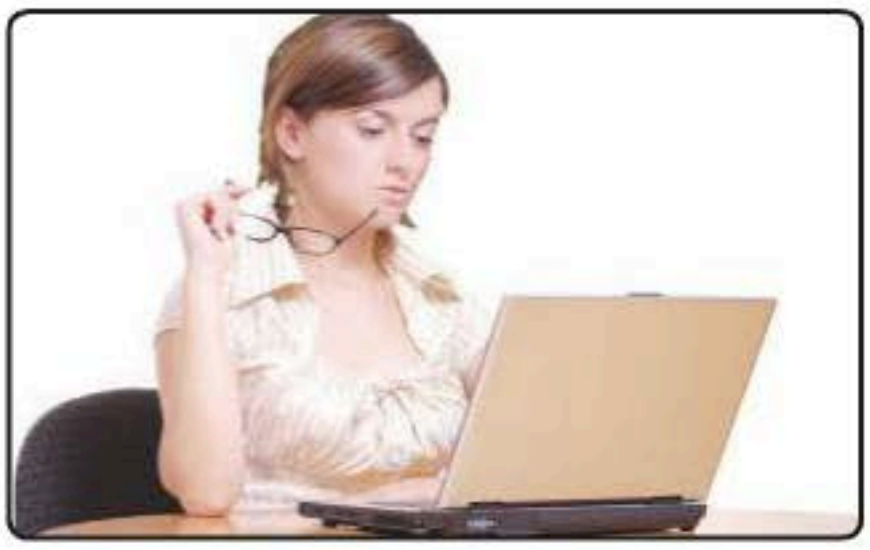


Figura 2. **La empresa debe responder civilmente por las acciones de sus empleados.**

acciones de sus empleados. Por lo tanto, cuando el administrador de la red es empleado, si alguna de sus acciones (u omisiones) causara un daño a terceros, dichos terceros seguramente demandarían a la empresa para la cual trabaja el administrador, y no, a este último. Más aún, en algunos casos, la normativa podría impedir que se demandara directamente al administrador cuando este sea dependiente.

Sin embargo, en este escenario, la responsabilidad que se ve acrecentada es la del administrador respecto de la empresa para la que trabaja. Porque si bien dicha empresa será responsable frente a los terceros, luego podrá reclamar civilmente al administrador para recuperar lo que hubiera pagado (además, por supuesto, del eventual despido que podría disponerse en el ámbito laboral).

EL ADMINISTRADOR DE LA RED COMO CONTRATISTA INDEPENDIENTE

En el caso del administrador de la red que no es empleado sino contratista independiente, su responsabilidad civil es amplia, tanto respecto de los terceros que pudieran resultar damnificados, como de la empresa titular de la red. Además, si el propio administrador de la red tuviera, a su vez, empleados, también es responsable por los actos de estos.

A continuación, analizaremos los presupuestos de la responsabilidad civil y cómo se aplican al administrador de la red.

Presupuestos de **la responsabilidad civil**

Para que exista responsabilidad civil deben darse los siguientes presupuestos:

1. Daño.

2. Antijuridicidad.

3. Factor de atribución.

4. Nexo de causalidad.

EL DAÑO

El **daño** es la lesión en los bienes (daño material) o en los sentimientos (daño moral) de una persona. Es el primer presupuesto de la responsabilidad civil, por lo que si no hay daño, no hay responsabilidad civil.

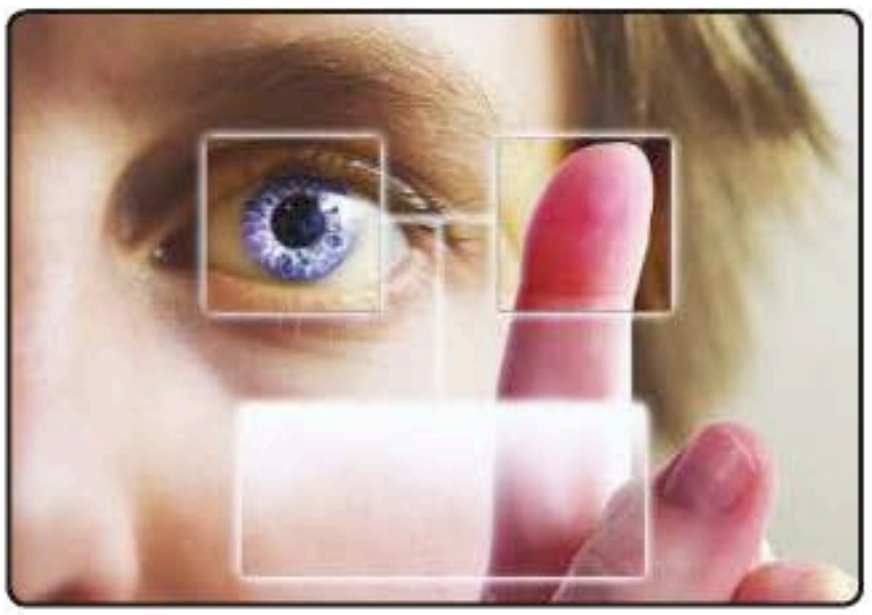


Figura 3. **El daño no necesariamente debe ser físico. También puede ser a los sentimientos.**

LA ANTIJURIDICIDAD

El segundo presupuesto es la **antijuridicidad** de la acción. Esto significa que la conducta de quien causa el daño debe ser **ilegítima**.

Ahora bien, es importante destacar que el concepto de antijuridicidad ha ido cambiando a lo largo del tiempo, y en la actualidad no se requiere que la acción sea ilegítima en sí, sino que basta con que sea **reprochable**. A modo de ejemplo, la conducta del administrador de una red que ha omitido instalar la actualización de un programa de seguridad no es, en sí misma, una conducta ilegítima, pero sí es reprochable. Y esto alcanza para que esté cumplido el requisito de antijuridicidad.

EL FACTOR DE ATRIBUCIÓN

El tercer presupuesto de la responsabilidad civil es el denominado **factor de atribución**. Se trata del fundamento por el cual se responsabiliza a quien realizó la conducta reprochable.

Este puede ser **subjetivo**, es decir, basado en la **culpa**; u **objetivo**, basado en el **riesgo** u otra circunstancia que resulta independiente de la voluntad de quien realiza la acción.

En materia de responsabilidad civil, el factor de atribución tradicional era subjetivo, basado en la culpa. Es decir, una persona tendría que responder civilmente únicamente si había existido un obrar **negligente**, **imprudente** o mediando **impericia** de su parte.

Ahora bien, con el desarrollo de la tecnología, el factor de atribución subjetivo comenzó a resultar insuficiente. En efecto, esto quedó en evidencia con la generalización del uso de los automóviles, porque existían casos en los cuales, a pesar de no existir culpa por parte del dueño del automóvil, se generaba un daño a un tercero. Y en estos casos, el sistema basado en el factor de atribución subjetivo no brindaba una solución justa para las víctimas. Fue entonces que se pensó en un factor de

EL FACTOR DE ATRIBUCIÓN Y LOS BUSCADORES DE INTERNET

Hace poco tiempo, Google fue condenado civilmente en la Argentina por la existencia de contenidos agraviantes subidos por terceros, aplicando el factor objetivo de atribución. Esta condena generó mucha preocupación en las empresas de Internet.

atribución distinto, **objetivo**, basado originalmente en el **riesgo**. El razonamiento fue el siguiente: quien introduce en la sociedad un elemento riesgoso, como lo es el automóvil, debe responder civilmente por los daños que este pueda causar.

EL NEXO DE CAUSALIDAD

Por último, resta mencionar el **nexo de causalidad**. Este presupuesto de la responsabilidad civil exige que exista una relación directa entre la conducta y el daño. Es decir, el daño debe haber sido causado como consecuencia de la conducta.

Siguiendo con el ejemplo que dimos respecto de la conducta reprochable, si como consecuencia de la falta de actualización del programa de seguridad por parte del administrador de la red, un hacker ingresara y generara algún daño a la información de los usuarios, existiría un claro nexo de causalidad entre la conducta del administrador y el daño ocasionado. Si el administrador de la red hubiera actualizado el programa de seguridad, el hacker no habría entrado y, por lo tanto, el daño no se hubiera causado.

RESUMEN SOBRE LOS PRESUPUESTOS DE LA RESPONSABILIDAD CIVIL

A continuación, detallamos las principales características de los presupuestos de la responsabilidad civil que explicamos en este capítulo.

PRESUPUESTOS DE LA RESPONSABILIDAD CIVIL	
Daño	Para que exista responsabilidad civil debe haberse ocasionado un daño. El daño es la lesión en los bienes o sentimientos de una persona.
Antijuridicidad	La conducta que ocasionó el daño debe ser reprochable. Este criterio se ve atenuado cuando el factor de atribución es objetivo, porque en tal caso, la voluntad de quien realiza la conducta no resulta relevante.
Factor de atribución	Es el fundamento por el cual se responsabiliza a quien realizó la acción reprochable que ocasionó el daño. Puede ser subjetivo, atendiendo a la culpa de la persona que efectuó la acción; u objetivo, atendiendo al riesgo creado.
Nexo de causalidad	Es la relación directa que debe existir entre la conducta reprochable y el daño ocasionado. Este requisito es menos importante cuando estamos ante un factor de atribución objetivo.

Tabla 1. Resumen de los presupuestos de la responsabilidad civil.

Responsabilidad **civil aplicable al administrador**

Hasta aquí hemos descripto, en términos generales, los presupuestos de la responsabilidad civil. A continuación, nos referiremos, específicamente, al régimen que resulta aplicable al administrador de la red, dejando aclarado que en la actualidad existe una importante discusión sobre la responsabilidad civil en materia tecnológica.

Si como consecuencia de alguna actividad ocurrida en la red se produjera un **daño** (primer presupuesto de la responsabilidad civil), debería analizarse si la responsabilidad por dicho daño puede ser imputada al administrador de la red. Para esto, básicamente, deben repasarse los presupuestos de la responsabilidad civil.

Ante todo, debemos señalar que, desde el punto de vista jurídico, el administrador de la red es un **profesional**. Por lo tanto, su conducta se evaluará con estándares más estrictos que la de cualquier persona que no tenga su nivel de conocimiento.

Para saber si el administrador de la red ha incurrido en una acción **reprochable** (que es el segundo presupuesto de la responsabilidad civil) se analizará su conducta comparándola, en abstracto, con la conducta esperable para un profesional que hubiera estado en la misma situación. Ahora bien, lo más importante para poder evaluar la responsabilidad civil del administrador es determinar si resulta aplicable el factor de atribución subjetivo o, por el contrario, nos encontramos ante un régimen objetivo.

En este sentido, debemos señalar que, en principio, el régimen de responsabilidad profesional es de carácter **subjetivo**. Es decir, los profesionales en general solo responden cuando han obrado con culpa, y esto sería aplicable al administrador de la red.

Por lo tanto, para eximirse de responsabilidad, el administrador de la red deberá demostrar que actuó con plena diligencia, adoptando todas las medidas que resultaban exigibles, según el estado de la técnica y sus conocimientos específicos, para evitar el daño.

Sin embargo, debemos señalar que en el último tiempo ha surgido una importante corriente

EL CONCEPTO DE CASO FORTUITO

Consiste en un evento que impide el cumplimiento de la obligación y que no ha podido preverse o que, previsto, no ha podido evitarse. Un ejemplo de esto podría ser un terremoto o un tsunami, que interrumpen las comunicaciones en una red.

de pensamiento, que considera que la actividad informática es una **actividad riesgosa**. Si esto fuera así, entonces el factor de atribución será objetivo, y ya no se tendrá en cuenta si el administrador de la red ha actuado con culpa o no: sería responsable por el solo hecho de ser el administrador de la red en la que se causó el daño.

En este caso, el administrador de la red únicamente podría eximirse de responsabilidad acreditando que:

1. No existe nexo causal entre el hecho y el daño (en nuestro ejemplo, que el daño no se debió a alguna acción ocurrida en la red).

2. Existió culpa de la víctima.

3. Concurre alguna situación de caso fortuito.

Como puede apreciarse, si los tribunales comienzan a adoptar esta idea de que la actividad informática es peligrosa, las contingencias en materia de responsabilidad civil para quienes administren las redes se verán incrementadas sustancialmente.

Por último, siguiendo con nuestro análisis, para verificar si podría existir responsabilidad del administrador de la red, debería analizarse el **nexo de causalidad** entre su conducta y el daño ocasionado.

Con relación a esta última cuestión, la actividad informática muchas veces genera inconvenientes interpretativos. Es que, en el ámbito físico, es mucho más sencillo probar la relación de causalidad que en el ámbito virtual.

EJEMPLOS PRÁCTICOS DEL ANÁLISIS DE LA RESPONSABILIDAD CIVIL

A continuación, veremos dos ejemplos prácticos respecto de cómo se analizaría la responsabilidad civil en un hecho ocurrido en el mundo físico y, luego, en un hecho ocurrido en el ámbito virtual.

Ámbito físico

El primer ejemplo es sobre algo muy simple y que ocurre a diario. Supongamos que una persona patea una pelota y rompe el vidrio de un vecino. El análisis de su responsabilidad civil es muy sencillo:

1. El **daño** es patrimonial, y consiste en el valor de ese vidrio, más los eventuales perjuicios que pudiera haber ocasionado con su rotura.

2. La **antijuridicidad** está dada por la conducta **reprochable** de haber pateado la pelota sin tener en cuenta las distancias o calculando mal.

3. El **factor de atribución** es **subjetivo** y, en este caso, se basa en la **imprudencia** de quien pateó la pelota.

4. El **nexo de causalidad** es muy claro: si la persona no pateaba la pelota, la pelota no golpeaba el vidrio, y si eso no ocurría, no había daño alguno.

Ámbito virtual

Ahora, realizaremos el mismo análisis pero referido a la conducta del administrador de una red. El administrador omitió aplicar un parche de seguridad en el sistema de validación de

usuarios, que determinó que quienes tuvieran sus computadoras infectadas con un malware determinado vieran comprometidas sus credenciales de acceso a la red:

1. El **daño** consiste en la pérdida de información y/o de la violación de la privacidad de los usuarios que vieron comprometidas sus credenciales de acceso. Corresponderá efectuar la cuantificación de este daño en un tribunal judicial.

2. La **antijuridicidad** está dada por la conducta **reprochable** del administrador de la red, que omitió aplicar el parche de seguridad.

3. El **factor de atribución** es **subjetivo** y, en este caso, se basa en la **impericia** del administrador, que en su condición de profesional, no podía ignorar que debía aplicarse un parche de seguridad.

4. El **nexo de causalidad** no es tan claro, o al menos podría ser cuestionado, porque la realidad es que solo resultaron afectados los usuarios que ya tenían infectadas sus máquinas. Es decir, si esas máquinas no hubiesen estado infectadas con el malware, entonces no habría habido consecuencias negativas de la conducta reprochable del administrador de la red. En este caso, en la relación de causalidad confluyen dos situaciones, una de las cuales es imputable al administrador de la red, pero la otra no.

Estos dilemas con el nexo de causalidad son muy comunes en el ámbito de la tecnología, y muchas veces resultan imposibles de probar (por ejemplo, cuando una computadora falla, a veces no puede determinarse si eso se debió al hardware, al software o a ambos, con lo cual se complica el análisis de la responsabilidad civil).

Cómo limitar la **responsabilidad civil del administrador**

En este punto nos referiremos a distintas acciones que el administrador de la red debería de tener en cuenta a fin de atenuar o limitar su responsabilidad civil.

Es importante dejar aclarado que enunciaremos estándares de conducta generales, que deberán ser evaluadas en cada caso de acuerdo con la legislación que resulte aplicable. Además, algunas de estas acciones se referirán al administrador de la red que, a la vez, es empleado; mientras que otras estarán dirigidas al administrador de la red que es contratista independiente.

REDACTAR POLÍTICAS CLARAS DE USO DE LA RED

Sin dudas, la primera acción que resulta recomendable es procurar que la red tenga **políticas claras de utilización**, que deben ser **notificadas** a todos los usuarios, y cuyo cumplimiento debe ser exigido por el administrador de la red.

Si el administrador es un empleado de la empresa titular de la red, entonces debería requerir a dicha empresa la redacción de las políticas. En caso de que fuese un contratista independiente, tal vez él mismo debería redactar las políticas. Pero en cualquier caso, la existencia de políticas de uso claras de la red beneficiará la evaluación de las conductas del administrador (de hecho, la inexistencia de políticas evidenciaría, de por sí, una conducta negligente del administrador).

Ahora bien, ¿qué deben contener estas políticas para que resulten útiles a los fines de demostrar la diligencia del administrador de la red? En términos generales, podemos decir que las políticas deben establecer:

1. Con qué finalidad los usuarios deben utilizar la red, y las limitaciones a su uso, si las hubiera.

2. Qué actividades no se pueden realizar en la red, con el mayor grado de detalle para evitar que pueda entenderse que alguna actividad no estaba prohibida cuando, en realidad, sí lo estaba.

3. Qué facultades de control tiene el administrador de la red, y cuál es el ámbito de privacidad de los usuarios, si lo hubiera (por ejemplo, debería aclararse si el administrador puede acceder a las claves de los usuarios o si no puede hacerlo).

4. Cuáles son las consecuencias de violar las políticas de uso.

5. Debería existir una previsión específica relacionada con los derechos de propiedad intelectual, dado que son los que más comúnmente se violan a través de las redes de computadoras.

Por otra parte, es fundamental que las políticas sean **notificadas** a los usuarios, de modo tal que quede **alguna constancia** de ello que permita probar ante terceros (por ejemplo, un tribunal) que estas fueron notificadas.

En aquellas jurisdicciones en las que se ha implementado la firma digital o electrónica, sería ideal que la notificación de las políticas se realizara con este procedimiento. Y para las jurisdicciones en las que aún no está implementada, deberían al menos conservarse los registros o logs que permitan acreditar la notificación.

SEGUROS

Hasta hace poco tiempo, no era posible asegurar los riesgos derivados de la actividad informática. El seguro es el método más fácil de cobertura en caso de que se decida aplicar la responsabilidad objetiva a la actividad informática.

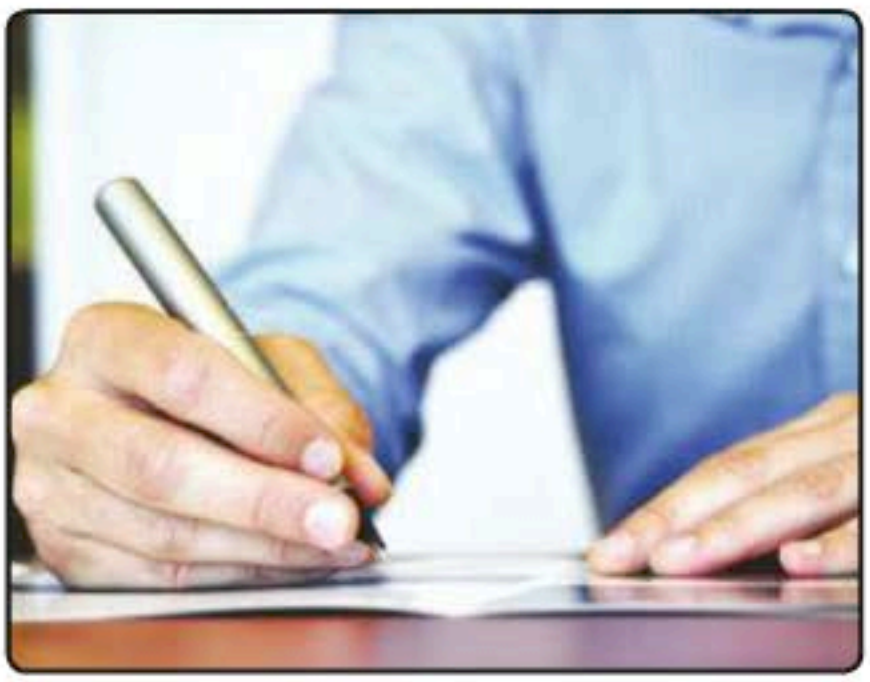


Figura 4. **Para limitar la responsabilidad del administrador es fundamental la redacción de políticas de uso.**

REQUERIR INSTRUCCIONES ESCRITAS PARA REALIZAR TAREAS QUE PUEDAN CONSIDERARSE VIOLATORIAS

Esta acción resultará aplicable, sobre todo, a los administradores de redes que son, a su vez, empleados de la empresa titular de la red que administran.

Estos administradores muchas veces se encuentran en situaciones complejas, porque no existen normas claras en la empresa respecto de su actuación, y reciben órdenes –que deben cumplir–, pero que podrían comprometer su responsabilidad personal. Un ejemplo claro sería el de una auditoría de correos electrónicos u otro tipo de comunicaciones internas.

Como vimos en el Capítulo 3, la violación del correo electrónico es un delito penal, y las empresas no pueden cometer delitos penales. Por lo tanto, si la auditoría pudiera ser considerada un delito, el administrador de la red sería el **autor material** (por lo menos, en principio) de dicho delito. Entonces, si bien entendemos que en el caso de la auditoría no debería haber problemas porque se trataría de correos electrónicos laborales (a los cuales, como vimos en el Capítulo 4, el empleador tiene derecho a acceder), lo cierto es que resultaría conveniente que el administrador de la red tuviera instrucciones escritas de sus superiores antes de realizar tales tareas.

Es importante aclarar que la instrucción escrita de un superior jerárquico en una empresa no eximirá al administrador de la red de su eventual responsabilidad penal si comete un delito, siempre que este sea evidente. Por ejemplo, si la empresa encomienda al administrador de la red que, aprovechando su acceso a información confidencial de los usuarios, monitoree el uso de las cuentas de correo electrónico personal de dichos usuarios, el administrador debería negarse, porque esa conducta constituye un delito penal.

SUSCRIBIR ACUERDOS DE CONFIDENCIALIDAD CON EMPLEADOS

En este caso, nos referiremos a una acción aplicable a los administradores que no son empleados, sino contratistas independientes. Como vimos, ellos son, a su vez, responsables por las acciones de sus propios empleados. Por lo tanto, resulta conveniente que suscriban con ellos acuerdos específicos de confidencialidad, dado que cualquier filtración de información que pudiera darse por los empleados del administrador será imputable directamente a él.

CLÁUSULAS DE LIMITACIÓN DE LA RESPONSABILIDAD O ACUERDOS DE INDEMNIDAD

Esta acción será útil tanto para el administrador de la red que es empleado como para el que es contratista independiente del titular de la red. Se trata de una acción fundamental porque tiene como finalidad limitar a un monto cierto y previsible la responsabilidad civil asumida por el administrador de la red.

En el caso del administrador que es empleado, es conveniente que requiera la suscripción de un acuerdo de indemnidad con la empresa. En algunos casos, dependiendo de la jerarquía del administrador dentro de la organización, y del tamaño de la organización, estos acuerdos se pueden firmar directamente con los dueños (por ejemplo, los accionistas extranjeros si se trata de una empresa multinacional que tiene una empresa chica en el país). El objeto de estos acuerdos es que la empresa o sus accionistas mantengan indemne al administrador ante cualquier reclamo que pudieran formular terceros por daños y perjuicios. Es decir, si el administrador de la red fuera demandado, y eventualmente condenado por considerarlo responsable civilmente de algún daño, la empresa (o sus accionistas) pagarían lo que corresponda para liberarlo de toda responsabilidad patrimonial. Es importante aclarar que estos acuerdos de indemnidad solo se refieren a los aspectos patrimoniales de la responsabilidad. Esto significa que, si el administrador de la red fuera imputado por un delito, y eventualmente condenado, **nadie podría sustituirlo** en el cumplimiento de la condena. Lo que suele acordarse para estos casos es que la empresa tomará a su cargo los eventuales gastos de defensa.

En el caso del administrador de la red que es un contratista independiente, resultaría conveniente que, en su contrato con la empresa titular de la red, acordara una cláusula limitativa de la responsabilidad civil.

En este sentido, dado que la responsabilidad civil, como dijimos, es de índole patrimonial, casi todas las legislaciones admiten que las partes puedan limitarla libremente. No ocurre así, por ejemplo, con la responsabilidad penal, que no podría limitarse.

Entonces, lo que el administrador puede pactar con la empresa titular de la red es que la responsabilidad civil del administrador, por todo

CORREO ELECTRÓNICO LABORAL Y DELITO

Algunos juristas sostienen que el empleador no tiene facultades para acceder al correo electrónico laboral sin orden de un juez. Por lo tanto, aun cuando pensemos en sentido contrario, alguien podría formular una denuncia para que un juez definiera el tema.

concepto, no exceda de un monto determinado. Esta limitación, cabe señalar, solo tendrá efecto entre las partes, lo que significa que terceros podrían demandar al administrador y, entonces, no se aplicaría el tope previsto contractualmente. Para estos casos, podría pactarse, además del límite contractual, una obligación de indemnidad de la empresa hacia el administrador, según la cual la empresa se comprometa a mantenerlo indemne de cualquier reclamo de terceros vinculado a su condición de administrador.

REALIZAR DENUNCIAS ANTE LA EVIDENCIA DE UN DELITO PENAL

Por último, es fundamental que el administrador de la red formule las **denuncias pertinentes** al verificar incumplimientos de las políticas de uso de la red o, en su caso, al comprobar la existencia de algún delito.

En el caso de incumplimientos de las políticas de uso de la red, el administrador –ya sea en su condición de empleado o de contratista independiente– debería dar inmediato aviso a la empresa para que esta tome los recaudos que considere. Para resguardar la responsabilidad del administrador, sería conveniente que estas comunicaciones se efectuaran por escrito, de modo tal que puedan probarse.

En caso de que el administrador verificase la comisión de algún delito en la red (por ejemplo, si que algún usuario está cometiendo delitos contra la propiedad intelectual), si es empleado tendría que informarlo por escrito, recomendando que se realice la correspondiente denuncia penal para deslindar responsabilidades. Si es contratista independiente, también debería informarlo por escrito, pero si advirtiera que la empresa se muestra permisiva con tales conductas, tendría que evaluar la posibilidad de realizar él mismo la denuncia penal correspondiente.

Esto dependerá, en gran medida, del delito de que se trate, pero podría ocurrir, por ejemplo, que el administrador advierta que algún usuario está distribuyendo pornografía infantil. Si la empresa no hiciera nada al respecto, luego podrían ser todos imputados por facilitar la comisión de ese delito, o bien por encubrirlo.

RESUMEN

El administrador de la red debe extremar las precauciones para evitar que, ante un evento dañoso, se le pueda endilgar responsabilidad por negligencia. Asimismo, debe procurar asegurarse de que su responsabilidad civil se encuentre limitada contractualmente.

Capítulo 6

Anexo documental

Veremos algunas normas, sitios de Internet y pronunciamientos judiciales relevantes.

RedUSERS.com

Anexo **documental**

En este último capítulo brindaremos algunas herramientas para profundizar los conocimientos respecto de los temas vistos anteriormente en el libro.

Con esta finalidad, presentaremos un listado de sitios web que podrían resultar de utilidad para obtener información legal **gratuita** y **confiable**. En este sentido, si bien en Internet existen innumerables sitios y foros de discusión sobre temas legales, en muchos de ellos la información no es fiable (por ejemplo, citan leyes que se encuentran desactualizadas o que, directamente, no existen).

Además, incluiremos un listado de las **principales normas** vinculadas a la temática vista en esta obra, de modo tal que el lector que así lo desee pueda profundizar en el estudio de estos temas.

Sitios **web**

A continuación, nos referiremos a los sitios web en que se puede encontrar información gratuita y, a la vez, confiable, respecto de los temas tratados en los capítulos precedentes.

PROTECCIÓN DE DATOS PERSONALES Y PRIVACIDAD

La temática vinculada a la protección de los datos personales ha sido una de las más desarrolladas en Internet, desde que la Comunidad Europea puso énfasis en este tipo de regulación. Por lo tanto, existe una gran cantidad de sitios dedicados a su análisis y discusión. Aquí presentaremos aquellos que consideramos más relevantes, aclarando que –como todo lo que se encuentra en Internet– este listado constituye solo un punto de partida para cualquier investigación, que debe ser actualizado en forma constante.

Sitios oficiales

Dirección Nacional de Protección de Datos Personales de la República Argentina:
www.jus.gob.ar/datos-personales.aspx

Agencia Española de Protección de Datos:
www.agpd.es/portalwebAGPD/index-ides-idphp.php

Unidad Reguladora y de Control de Datos Personales de Uruguay:
www.datospersonales.gub.uy

Autoridad Nacional de Protección de Datos Personales de Perú:
www.minjus.gob.pe/proteccion-de-datos-personales

Instituto Federal de Acceso a la Información y Protección de Datos de México:
www.ifai.org.mx

Sitios de ONGs o grupos de investigación sobre datos personales y privacidad

Electronic Privacy Information Center:
www.epic.org

Revista electrónica del Centro de Protección de Datos Personales de la Defensoría del Pueblo de la Ciudad de Buenos Aires:
www.habeasdata.org.ar

Electronic Frontier Foundation:
www.eff.org

DELITOS INFORMÁTICOS

A continuación, listaremos algunos sitios web que contienen información sobre delitos informáticos y cuestiones vinculadas.

Portal de información sobre delitos informáticos:
www.delitosinformaticos.com

Sitio web de un fiscal argentino especializado en delitos informáticos
www.ricardosaenz.com.ar

Grupo de Delitos Telemáticos, Guardia Civil de España:
www.gdt.guardiacivil.es/webgdt/home_alerta.php

Departamento de Ciberdelito del FBI:
www.fbi.gov/about-us/investigate/cyber/cyber

Departamento de Ciberdelincuencia de INTERPOL:
www.interpol.int/es/Internet/Criminalidad/Delincuencia-inform%C3%A1tica/Ciberdelincuencia

Cibercrimen, Consejo de Europa:
www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp

DERECHO DEL TRABAJO Y NUEVAS TECNOLOGÍAS

A continuación, algunos sitios web que contienen información sobre el Derecho del Trabajo y la tecnología y el trabajo.

Organización Internacional del Trabajo (OIT):
www.ilo.org/global/lang--es/index.htm#a3

Sociedad Argentina de Derecho Laboral:
www.laboral.org.ar/index.html

Sociedad Internacional de Derecho del Trabajo y la Seguridad Social:
http://asociacion.org.ar/ISLLSS/espanol/index_esp.htm

Asociación de Abogados Laboralistas:
http://www.aal.org.ar/.

PUBLICACIONES GENERALES CON CONTENIDO JURÍDICO

En este apartado listaremos algunos sitios jurídicos, con acceso gratuito, en los que se pueden encontrar noticias, opiniones, jurisprudencia y legislación sobre los temas tratados en esta obra.

El Dial (diario jurídico):
www.eldial.com.ar

Abogados.com.ar:
www.abogados.com.ar

Corte Suprema de Justicia de la Nación (Argentina):
www.csjn.gov.ar

Centro de Información Judicial, Agencia de noticias del Poder Judicial (Argentina):
www.cij.gov.ar

Diario Judicial (diario jurídico):
www.diariojudicial.com.ar

Red El Derecho Informático (Iberoamérica):
www.elderechoinformatico.com

FindLaw (EE.UU.):
www.findlaw.com

BUSCADORES DE NORMATIVA

En este apartado nos referiremos a buscadores de normativa, que son sitios en los que pueden encontrarse versiones oficiales o confiables de las normas vigentes en los diversos países.

Infoleg (Argentina):
http://infoleg.mecon.gov.ar

Diario Oficial de la Federación Mexicana:
http://dof.gob.mx/index.php

Agencia de Gobierno Electrónico y Sociedad de la Información (Uruguay):
www.agesic.gub.uy

Eur-Lex (Unión Europea):
http://europa.eu/eu-law/legislation/index_es.htm

ORGANISMOS INTERNACIONALES

A continuación, algunos sitios de organismos internacionales, que tienen contenido jurídico asociado a tratados u otros instrumentos internacionales que regulan aspectos del Derecho Informático.

Organización Mundial de la Propiedad Intelectual (OMPI):
www.wipo.org

Internet Corporation for Assigned Names and Numbers (ICANN):
www.icann.org/es/all

Organización para la Cooperación Económica y el Desarrollo:
www.oecd.org

Organización de los Estados Americanos (OEA):
www.oas.org/es/default.asp

Normativa **local**

En esta sección, listaremos las normas que, en diversos países, regulan los temas que hemos tratado en este libro. Este listado es meramente enunciativo, no pretende agotar la regulación existente en todos los países, sino brindar un primer acercamiento a las principales normas.

ARGENTINA

Ley de Protección de Datos Personales y Habeas Data N° 25326

Decreto Reglamentario de la Ley de Protección de Datos Personales y Habeas Data N° 1558/2001

Ley de Firma Digital Nº 25.506

Decreto Reglamentario de la Ley de Firma Digital Nº 2628/2002

Ley de Contrato de Trabajo Nº 20.744

Ley de Delitos Informáticos Nº 26.388

Ley de Propiedad Intelectual Nº 11.723

BOLIVIA

Decreto Supremo Nº 28.168. Acceso a la Información Pública

Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación Nº 164

Ley Nº 1322 de Derecho de Autor

Decreto Supremo Nº 23.907, reglamentario de la Ley de Derecho de Autor

CHILE

Ley de Delitos Informáticos Nº 19.223

Ley de Protección de Datos Personales Nº 19.628

Ley de Propiedad Intelectual Nº 17.336

ESPAÑA

Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal

Real Decreto 1720/2007, reglamentario del desarrollo de la Ley Orgánica 15/1999

Ley Orgánica 10/1995 (Código Penal)

Ley 29/2003 de Firma Electrónica

Real Decreto Legislativo 1/1996. Ley de Propiedad Intelectual

MÉXICO

Ley Federal de Protección de Datos Personales en Posesión de los Particulares

Código Penal Federal

Ley Federal de Derecho de Autor

Ley de Firma Electrónica Avanzada

PARAGUAY

Ley de Protección de Datos Personales Nº 1682

Ley de Propiedad Intelectual Nº 1328/98

Decreto Nº 5.159, reglamentario de la Ley de Propiedad Intelectual

Ley Nº 1160/97 (Código Penal)

Ley de Firma Electrónica Nº 4017/10

URUGUAY

Ley de Protección de Datos Personales y Habeas Data Nº 18.331

Ley de Acceso a la Información Pública Nº 18. 381

Ley de Firma Electrónica Nº 18.600

Código Penal

Normas **internacionales**

A continuación, las principales normas internacionales que se han dictado en materia de Derecho Informático, Delitos Informáticos y Protección de la Propiedad Intelectual.

En este sentido, es importante aclarar que, a nivel global, la normativa que más ha avanzado es la referida al Derecho de Autor, lo que ha permitido que los delitos informáticos vinculados a la piratería de obras puedan ser perseguidos internacionalmente (a modo de ejemplo, cabe mencionar el reciente caso de MegaUpload, en el cual se inició una causa en los Estados Unidos que terminó en la detención del titular del sitio web **Megaupload.com**, que vivía en otro país).

- Tratado de la Organización Mundial de la Propiedad Intelectual sobre Derecho de Autor
- Convenio de Berna para la Protección de las Obras Literarias y Artísticas
- Convenio de París para la Protección de la Propiedad Intelectual
- Acuerdos de la Organización Mundial del Comercio sobre la Propiedad Intelectual (ADPIC)

Conclusión

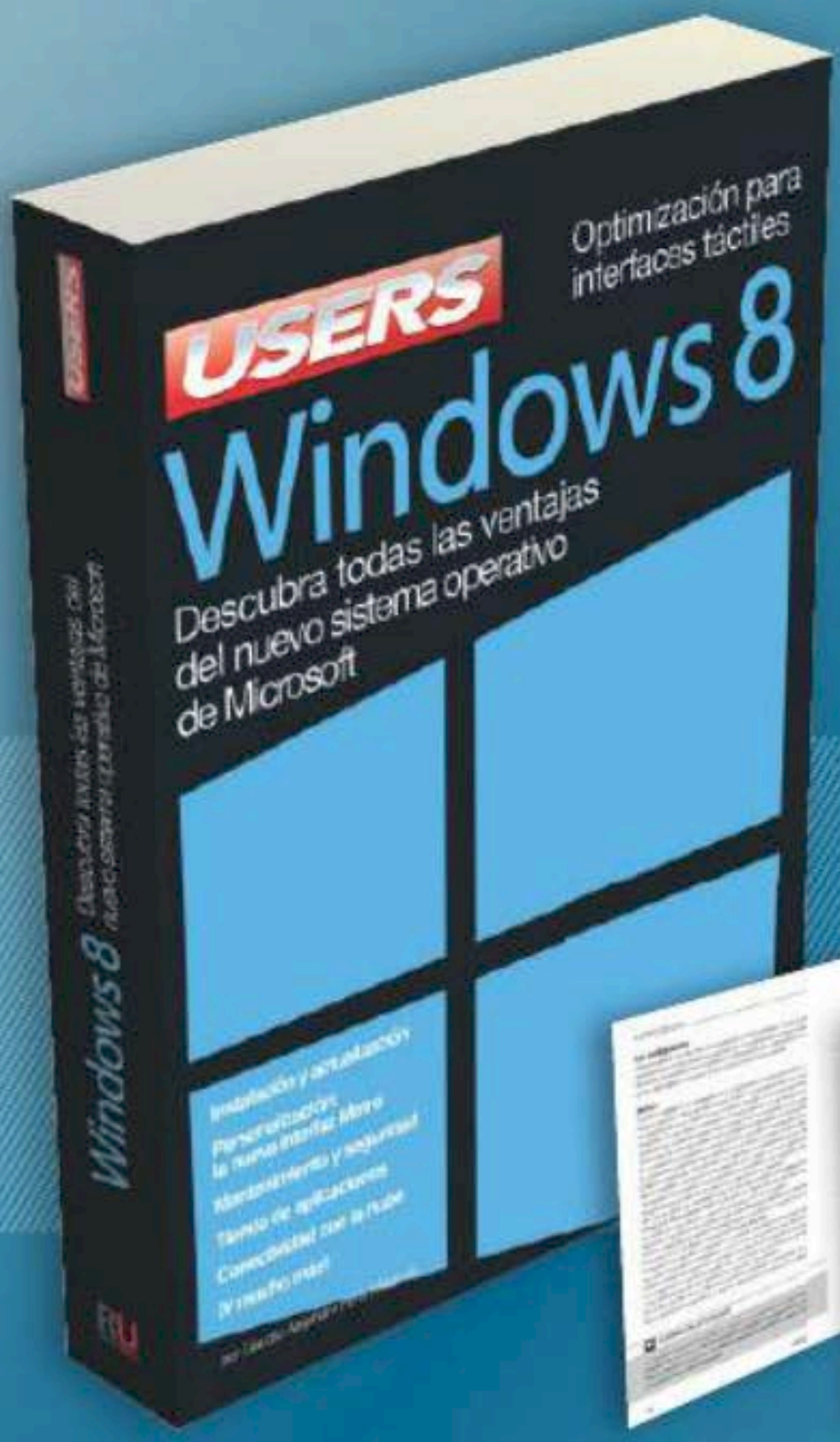
La aplicación de criterios jurídicos tradicionales a la actividad informática muchas veces genera incertidumbre. Las leyes previstas para el mundo físico se revelan como insuficientes para poder contemplar la gran cantidad de situaciones generadas como consecuencia del avance de la informática en nuestras vidas.

En este contexto, en el último tiempo se han dictado normas específicas que tienen en cuenta las particularidades de la actividad informática. Pero estas normas, a su vez, deben ser actualizadas constantemente, para seguir el ritmo de actualización de la informática.

Es por todo lo expuesto que la finalidad de este capítulo es brindar un buen punto de inicio para quien quiera adentrarse en la investigación de la informática jurídica. Probablemente, muchas de las normas que mencionamos estarán desactualizadas poco tiempo después de la publicación de esta obra. Pero el hecho de conocerlas servirá para acceder a aquellas que las sucedan en el futuro, por lo que consideramos oportuno listarlas.

Del mismo modo, los sitios de Internet que hemos incluido en este capítulo servirán, sin dudas, como disparadores para una búsqueda más profunda de contenidos jurídicos.

DESCUBRA TODAS LAS VENTAJAS DEL NUEVO SISTEMA OPERATIVO DE MICROSOFT



Luego del lanzamiento de un sistema operativo sólido y veloz como Windows 7, Microsoft ha desarrollado un nuevo sistema que presenta una interfaz renovada, disponible tanto para equipos de escritorio y portátiles, como para tablets. Esta obra nos permitirá descubrir esta novedad, junto a otros aspectos en términos de seguridad y rendimiento, para aprovechar el potencial de Windows 8 al máximo.

» MICROSOFT / WINDOWS
» 192 PÁGINAS
» ISBN 978-987-1857-67-8

LLEGAMOS A TODO EL MUNDO VÍA OCA * Y DHL **

* SÓLO VÁLIDO EN LA REPÚBLICA ARGENTINA // ** VÁLIDO EN TODO EL MUNDO EXCEPTO ARGENTINA

usershop.redusers.com // usershop@redusers.com

+54 (011) 4110-8700

USERS

Técnico en
REDES &SEGURIDAD

ASPECTOS LEGALES

Este interesante libro logra acercar al lector a todas las cuestiones jurídicas relacionadas al ámbito informático, tanto en el mundo real como en el virtual.
Se explican en profundidad temas fundamentales como la privacidad, los datos personales y su protección, la seguridad y confidencialidad de los usuarios y los delitos informáticos (daños, violación a la propiedad intelectual, estafas e intromisiones).
Sus capítulos están desarrollados de forma didáctica, con explicaciones sencillas y la mayor seriedad.

CONTENIDO

EXCLUSIVO PARA LECTORES

Profesores en línea:
profesor@redusers.com

Servicios para lectores:
usershop@redusers.com

9 789871 857777