CONFIDENCIALIDAD.

PROTECCION DE DATOS PERSONALES.

DERECHO A LA IMAGEN.

CONFIDENCIALIDAD

CONFIDENCIALIDAD

Definición de la RAE:

“Que se hace o se dice en la confianza de que se mantendrá la reserva de lo hecho o lo dicho.”

CONFIDENCIALIDAD

- Lo confidencial se relaciona con el secreto.
- Puede ser una estrategia de protección o una obligación legal.

CONFIDENCIALIDAD

- El secreto es una alternativa de protección en el campo de la propiedad intelectual.

- Se vincula mayoritariamente con la propiedad industrial y no tanto con el derecho de autor, donde lo confidencial se podría asociar con el derecho moral al inédito.

CONFIDENCIALIDAD

- En todo proceso de innovación o equipo de I+D, ante la obtención de un resultado relevante, se debe buscar una alternativa de protección.

- Esto es una decisión estratégica teniendo en cuenta varios factores, tipo y características del resultado, posibilidad de ingeniería inversa, etc.

CONFIDENCIALIDAD

Proteger por patente o por secreto tiene diferencias jurídicas sustanciales

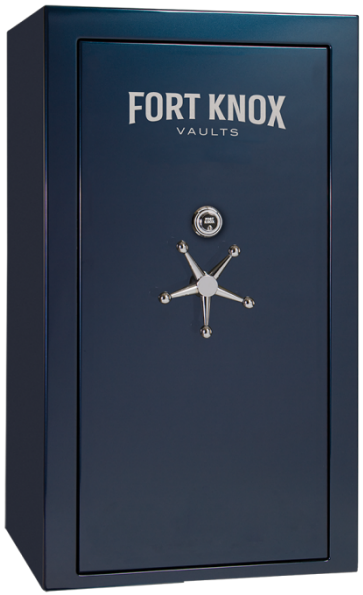
	PATENTE	SECRETO
Protección Legal	Se exigen novedad, altura inventiva, aplicación industrial	No se exige requisito alguno
Conocimiento del invento	Se revela mediante la publicación	No se revela, se mantiene en secreto
Título de propiedad	Se emite	No se emite
Derecho	Excluyente	No Excluyente
Extensión temporal	Definida (20 años desde la solicitud)	Indefinida (lo que dure el secreto)

CONFIDENCIALIDAD

Elegir la alternativa de protección más adecuada no es sencillo porque **equivocar la estrategia** puede implicar la **perdida del resultado**

CONFIDENCIALIDAD

El valor de la información

¿ 

?

El secreto mejor guardado…

CONFIDENCIALIDAD

El valor de la información

Patentar las formulas hubiera significado errores estratégicos MILLONARIOS !!!

CONFIDENCIALIDAD

Marco Normativo – Ley Nº 24.766

Art. 1º: Las personas físicas o jurídicas podrán impedir que la información que esté legítimamente bajo su control se divulgue a terceros o sea adquirida o utilizada por terceros sin su consentimiento de manera *contraria a los usos comerciales honestos*.

CONFIDENCIALIDAD

Marco Normativo – Ley Nº 24.766

Requisitos para que la información confidencial esté protegida:

- Que la información sea secreta (art. 1 inc. a)
- Que tenga un valor comercial por resultar secreta (art. 1 inc. b)
- Que haya sido objeto de razonables medidas de protección (art. 1 inc. c)

CONFIDENCIALIDAD

Marco Normativo – Ley Nº 24.766

"Art. 1º…Se considerará que es contrario a los usos comerciales honestos:

- el incumplimiento de contratos
- el abuso de confianza
- la instigación a la infracción
- la adquisición de información no divulgada, por terceros que supieran o no, por negligencia grave, que la adquisición implicaba tales practicas.

CONFIDENCIALIDAD

Marco Normativo – Ley Nº 24.766

Acciones Civiles:

Art. 11: (…) el acceso por terceros a la información de manera contraria a los usos comerciales honestos, dará derecho a quien la posea a ejercer las siguientes acciones civiles:

- Medidas cautelares
- Cese de uso
- Daños y perjuicios

CONFIDENCIALIDAD

Deber de confidencialidad en el Código Civil y Comercial de la Nación - Art. 992

Si durante las negociaciones, una de las partes facilita a la otra una información con carácter confidencial, el que la recibió tiene el deber de no revelarla y de no usarla inapropiadamente en su propio interés.

La parte que incumple este deber queda obligada a reparar el daño sufrido por la otra.

Si ha obtenido una ventaja indebida, queda obligada a indemnizar a la otra parte en la medida de su propio enriquecimiento.

CONFIDENCIALIDAD

Acciones penales – Ley Nº 24.766

Art. 12: “Quien incurriera en la infracción de lo dispuesto en la presente ley en materia de confidencialidad, quedará sujeto a la responsabilidad que correspondiera conforme con el Código Penal.”

CONFIDENCIALIDAD

Acciones penales – Ley Nº 24.766

Código Penal - Art. 156 - VIOLACIÓN DE SECRETOS

El que teniendo noticia, por razón de su estado, oficio, empleo, profesión o arte, de un secreto cuya divulgación pueda causar daño, lo revelare sin justa causa:

- multa de $ 1.500 a $ 90.000
- inhabilitación especial por 6 meses a 3 años

CONFIDENCIALIDAD
Laboral

CONFIDENCIALIDAD
Laboral

Ley de Confidencialidad - Ley Nº 24.766

Art. 3: alcanza a toda persona que con motivo de su trabajo, empleo, cargo, puesto, desempeño de su profesión o relación de negocios, tenga acceso a una información que sea considerada confidencial y sobre cuya confidencialidad se los haya prevenido.

CONFIDENCIALIDAD
Laboral

Ley de Contrato de Trabajo – DEBER DE FIDELIDAD

Art. 85 “El trabajador debe observar todos aquellos deberes de fidelidad que deriven de la índole de las tareas que tenga asignadas, guardando reserva o secreto de las informaciones a que tenga acceso y que exijan tal comportamiento de su parte”

CONFIDENCIALIDAD
Laboral

Los objetos pasibles de protección por secreto pueden ser:

- Hechos, producciones,
- Ideas, invenciones,
- Conocimientos, procedimientos técnicos, etc.

CONFIDENCIALIDAD
Académica

CONFIDENCIALIDAD
Académica

Toda aquella información que no es públicamente divulgada y que puede resultar de utilidad o causar un daño a la universidad, a profesores o alumnos.

CONFIDENCIALIDAD
Académica

Deber tácito en determinadas relaciones internas:

- Docentes y Alumnos
- Equipos de Investigación
- Profesores
- Empleados colaboradores
- El caso complejo de la publicación de trabajos de investigación

CONFIDENCIALIDAD
Académica

Buenas prácticas:

- Protección Contractual: Convenio de Confidencialidad y Cláusula de Confidencialidad
- Reglamento de Manejo de Información

CONFIDENCIALIDAD
Académica

Esquema de Convenio de Confidencialidad

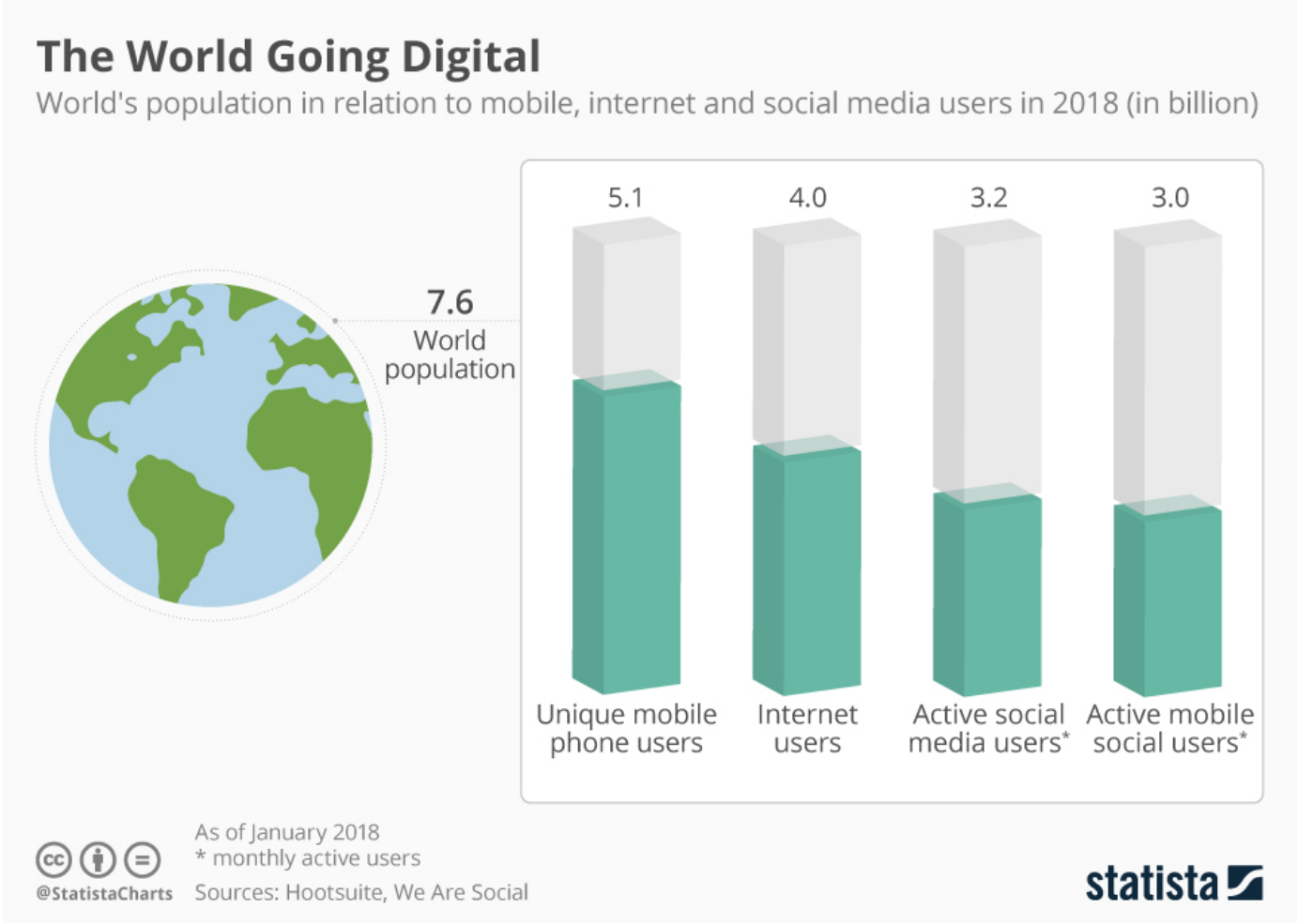
- Definición de información confidencial
- Información que no es confidencial
- Excepciones al deber de confidencialidad
- Plazo de duración
- Titularidad de la información
- Jurisdicción y Competencia en caso de conflicto

CONFIDENCIALIDAD
Académica

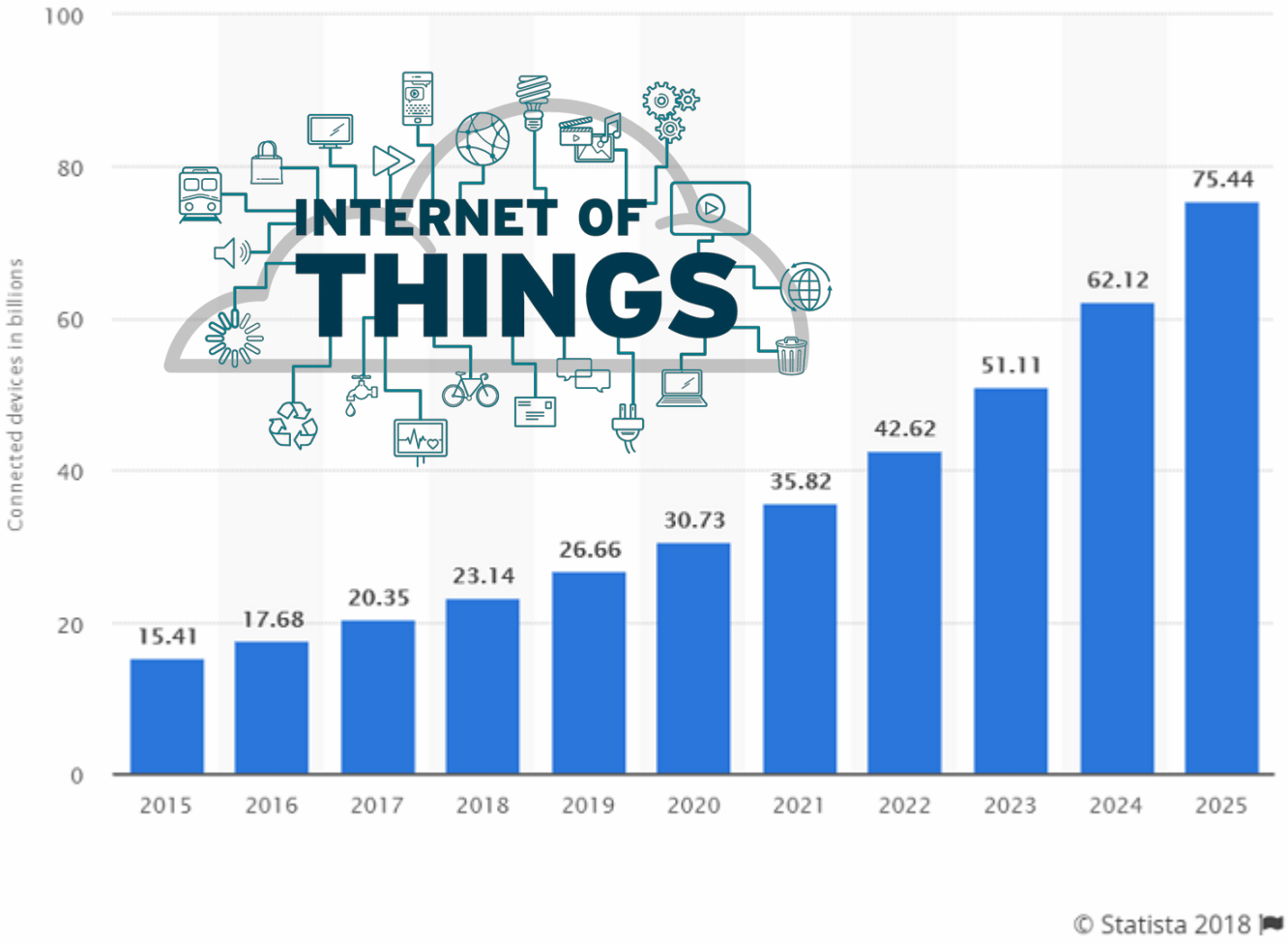
- Publicaciones y Presentaciones. La INSTITUCION o el INVESTIGADOR tendrán derecho a publicar los resultados obtenidos en la realización del Estudio siempre que, con una antelación no menor de sesenta (60) días a la publicación ("Divulgación de los Resultados del Estudio") la INSTITUCION o el INVESTIGADOR envíen a XXXX dicha Divulgación de los Resultados del Estudio para la revisión y comentarios de XXXXXX y para constatar si existe contenido patentable o Información Confidencial de XXXXXXXX dentro de la misma. XXXXXXXX devolverá los comentarios a la INSTITUCION o al INVESTIGADOR dentro de los sesenta (60) días de recibido el proyecto de Divulgación de los Resultados del Estudio ("Periodo de Revisión"). Además, la INSTITUCION o el INVESTIGADOR deberán postergar toda Divulgación de los Resultados del Estudio por otros sesenta (60) días más después del Período de Revisión, si así lo solicitara XXXXXXXXX, para permitirle asegurar la protección de la patente u otros derechos de propiedad ("Período de Postergación"). La INSTITUCION y el INVESTIGADOR aceptan mantener la Divulgación de los Resultados del Estudio en forma confidencial hasta tanto no haya caducado el Período de Revisión y el Período de Postergación, si fuera solicitado. La INSTITUCION o el INVESTIGADOR deberán dar la debida consideración a los comentarios efectuados por XXXXXXX. La INSTITUCION y el INVESTIGADOR aceptan eliminar la Información Confidencial de XXXXXXXXX de toda Divulgación de los Resultados del Estudio. En el caso de que la INSTITUCION o el INVESTIGADOR y XXXXXXXXXXX difirieran en sus opiniones o interpretación de los datos de la Divulgación de los Resultados del Estudio, las partes deberán resolver tales diferencias de buena fe a través de un debate científico apropiado.

CONFIDENCIALIDAD y Datos Personales

CONFIDENCIALIDAD
y Datos Personales



CONFIDENCIALIDAD
y Datos Personales



CONFIDENCIALIDAD y Datos Personales

2018: mas de la mitad de la población mundial conectada a internet mediante 23 mil millones de dispositivos conectados en todo el mundo.

2025: con el boom del Internet de las Cosas (IoT) se estima superar los 75 mil millones de dispositivos.

En 2016, el mercado de IoT movió USD 157 mil millones y se estima que llegará a generar USD 457 mil millones para 2020.

CONFIDENCIALIDAD y Datos Personales

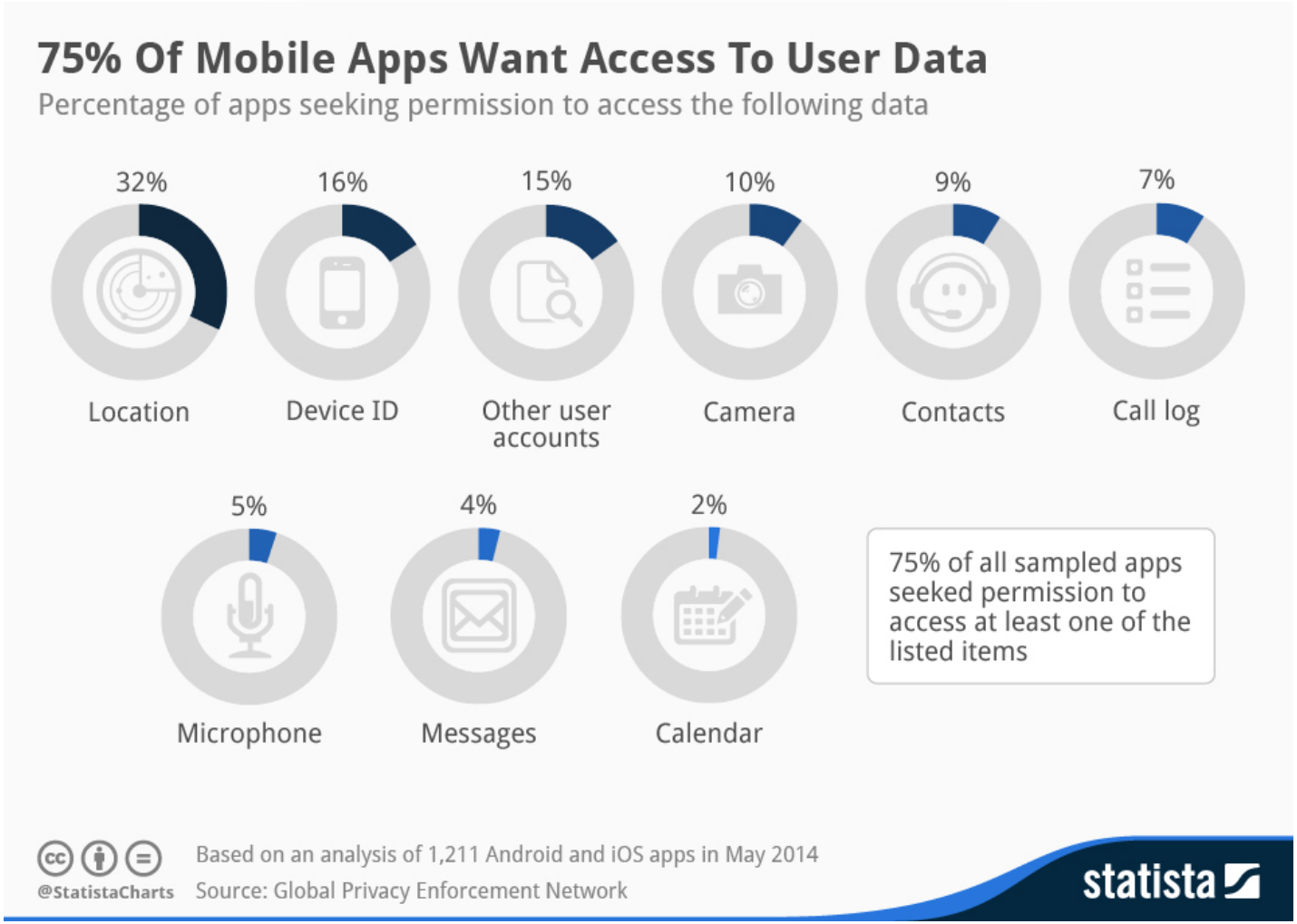
¿Y que tienen que ver los datos personales en esto?

Los datos personales son el **nuevo petróleo del siglo XXI.**

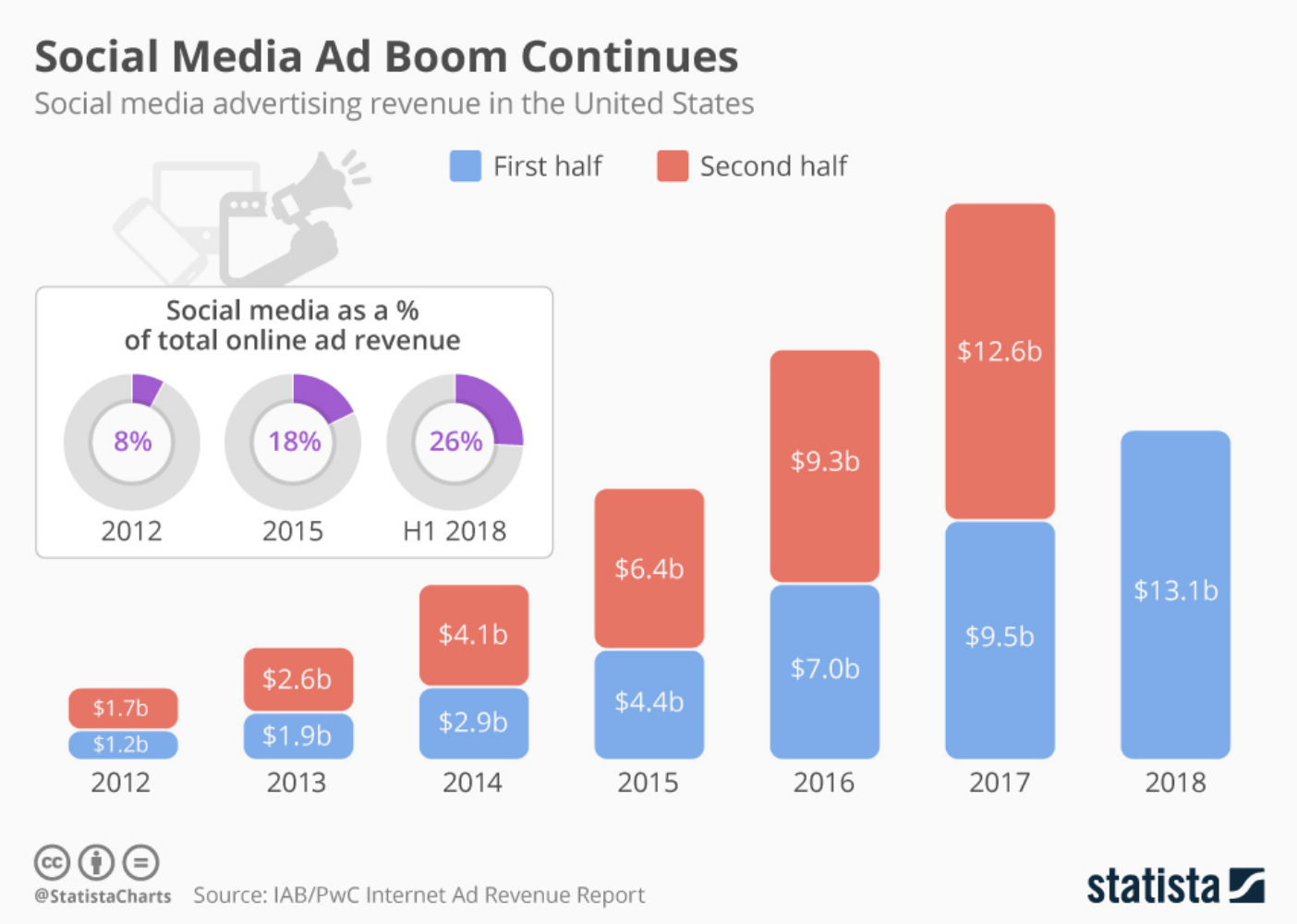
El flujo digital de información y datos personales está dando lugar a una nueva economía donde su rol es central.

CONFIDENCIALIDAD
y Datos Personales

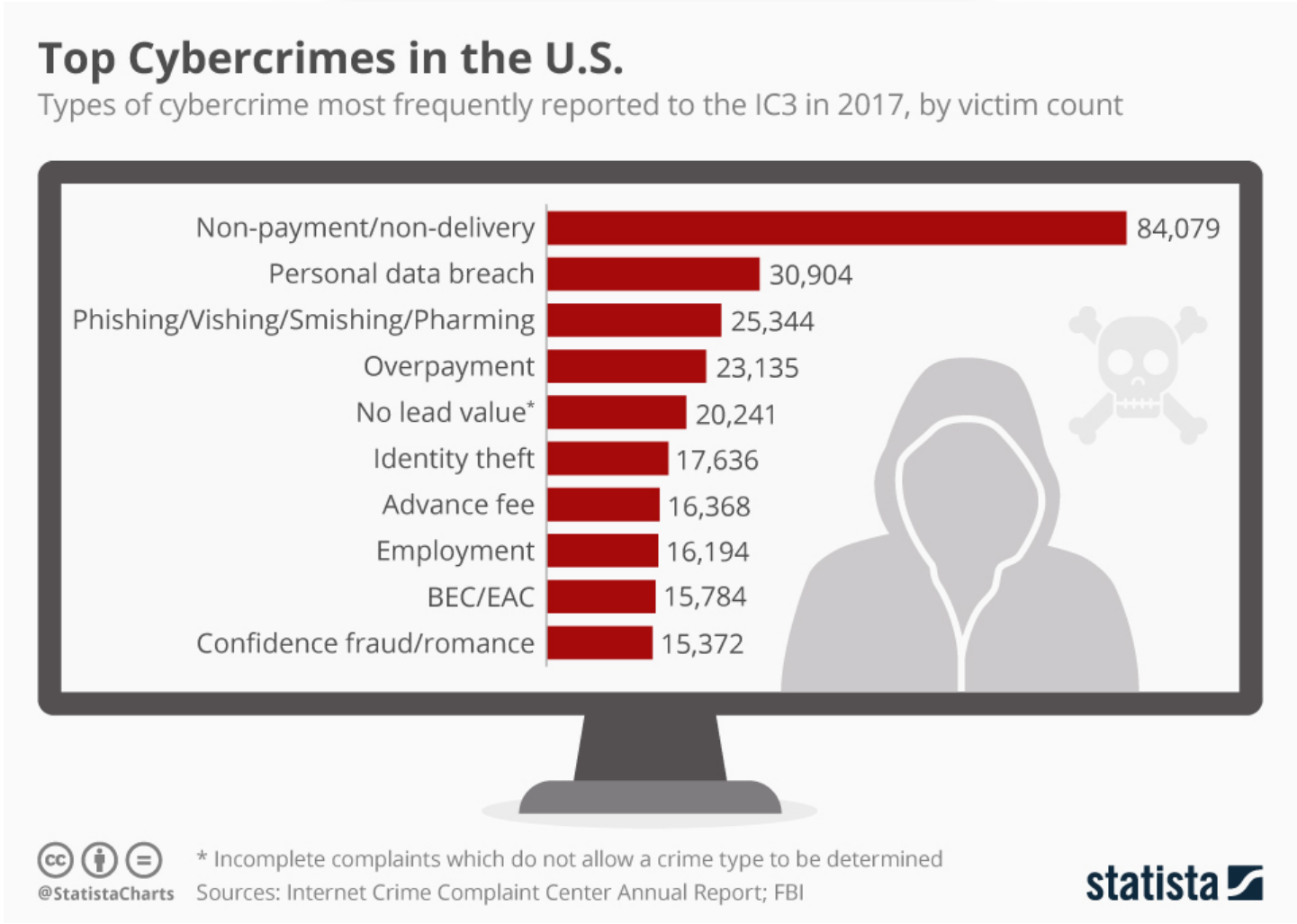
CONFIDENCIALIDAD y Datos Personales



CONFIDENCIALIDAD
y Datos Personales



CONFIDENCIALIDAD
y Datos Personales



CONFIDENCIALIDAD
y Datos Personales

RESUMEN LATINOAMERICANO

LA OTRA CARA DE LAS NOTICIAS DE AMÉRICA Y EL TERCER MUNDO

Caso Cambridge Analytica. Las redes no son gratis, las pagas con tus datos

En internet no existe la privacidad

ONLINE

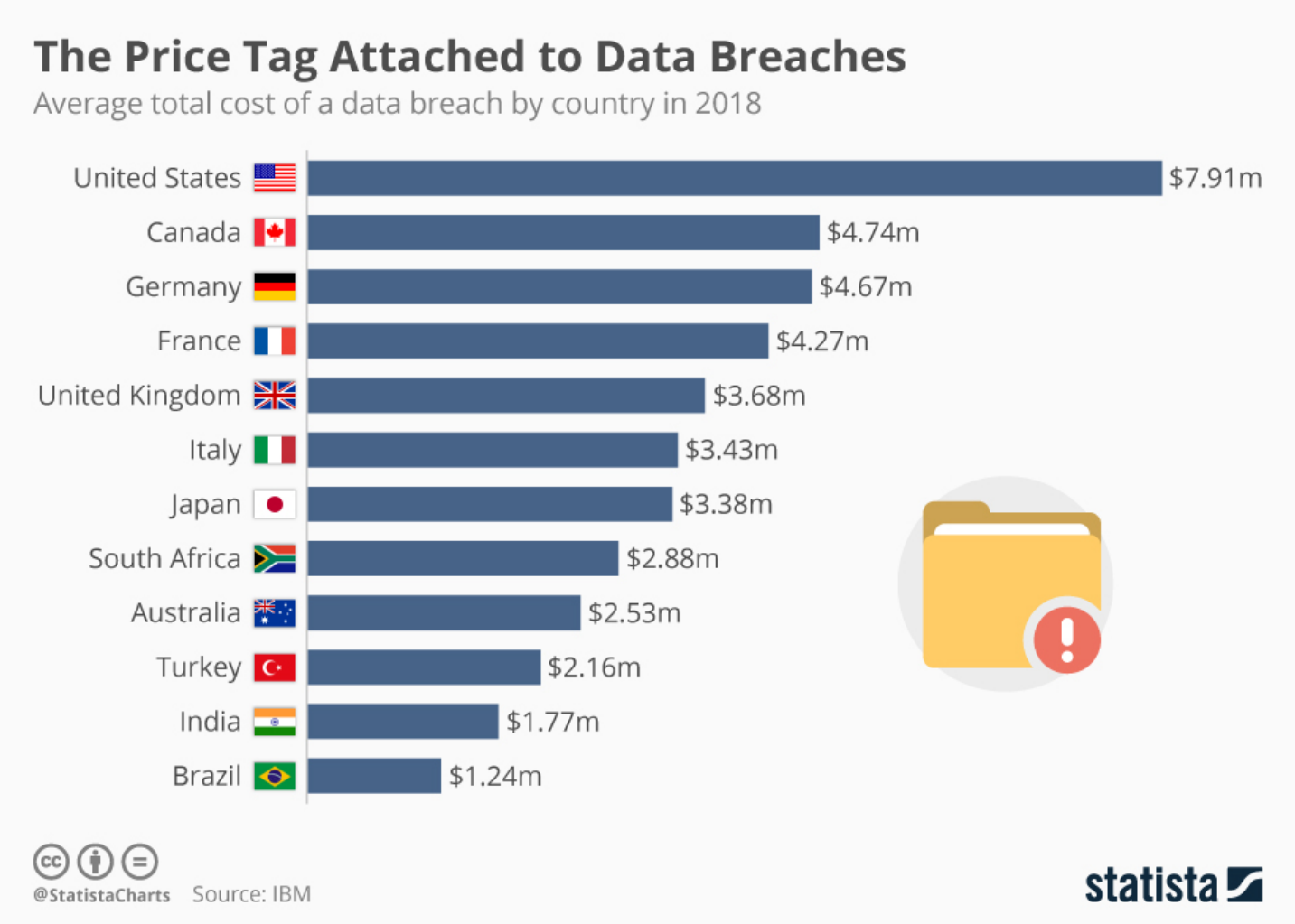
HACK
FACE

LO ADMITIÓ
PERO RECIÉN
28 de Septiem

Según el p
internos y
comerciar

SADO

CONFIDENCIALIDAD
y Datos Personales



CONFIDENCIALIDAD y Datos Personales

LEY Nº 25.326 - DE PROTECCIÓN DE DATOS PERSONALES

Objeto (art. 1): la protección de los datos personales asentados en archivos, registros, bancos de datos, públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre. (de conformidad con el art. 43 CN).

CONFIDENCIALIDAD y Datos Personales

Definiciones:

- **Datos personales**: información referida a personas físicas o de existencia ideal.

- **Datos sensibles**: datos 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.

- **Base o banco de datos**: conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, cualquiera que fuere la modalidad de almacenamiento o acceso

CONFIDENCIALIDAD y Datos Personales

Definiciones:

- **Tratamiento de datos**: operaciones y procedimientos que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos.

- **Responsable de la base o banco de datos:** persona física o de existencia ideal pública o privada, que es titular de la base o banco de datos.

CONFIDENCIALIDAD y Datos Personales

Definiciones:

- **Titular de los datos:** toda persona cuyos datos sean objeto del tratamiento.
- **Usuario de datos:** toda persona, que realice el tratamiento de datos, ya sea en bases de datos propias o a través de conexión con los mismos.
- **Disociación de datos:** todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada.

CONFIDENCIALIDAD y Datos Personales

PRINCIPIO DE CALIDAD DEL DATO (art. 4):

1. Los datos que se recojan deben ser ciertos, adecuados, pertinentes y no excesivos.

2. La recolección de datos no puede hacerse por medios desleales o fraudulentos.

3. Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles.

(SIGUE)

CONFIDENCIALIDAD y Datos Personales

4. Los datos deben ser exactos y actualizarse.

5. Los datos total o parcialmente inexactos, o incompletos, deben ser suprimidos y sustituidos.

6. Los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular.

7. Los datos deben ser destruidos cuando hayan dejado de ser necesarios.

CONFIDENCIALIDAD y Datos Personales

CONSENTIMIENTO (art. 5):

El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento **libre, expreso, informado y por escrito**.

No será necesario el consentimiento cuando:

a) Los datos se obtengan de fuentes de acceso público irrestricto;

b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal;

(SIGUE)

CONFIDENCIALIDAD y Datos Personales

c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio;

d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento;

e) Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes.

CONFIDENCIALIDAD y Datos Personales

DATOS SENSIBLES (art. 7):

1. Es prohibida la formación de bases de datos que almacenen información que directa o indirectamente revele datos sensibles. (Iglesia Católica, las asociaciones religiosas y organizaciones políticas y sindicales podrán tener registro de sus miembros, y los datos de antecedentes penales o contravencionales sólo pueden tratarlos las autoridades públicas competentes).

2. Nadie puede ser obligado a proporcionar datos sensibles.

3. Sólo pueden ser recolectados cuando haya sido autorizado por ley, o para finalidades puramente estadísticas o científicas con la debida disociación.

CONFIDENCIALIDAD y Datos Personales

DATOS DE SALUD (art. 8):

Los establecimientos sanitarios y los profesionales vinculados a la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento.

CONFIDENCIALIDAD y Datos Personales

DEBER DE SEGURIDAD (art. 9):

1. El responsable del archivo debe adoptar las medidas técnicas necesarias para garantizar la seguridad y confidencialidad de los datos personales y evitar su adulteración, pérdida, consulta o tratamiento no autorizado.

2. Queda prohibido registrar datos personales en bases de datos que no reúnan condiciones de seguridad.

CONFIDENCIALIDAD y Datos Personales

DEBER DE CONFIDENCIALIDAD (art. 10):

1. El responsable y las personas que intervengan en cualquier fase del tratamiento de datos están obligados al secreto profesional.

2. Podrá ser relevado por resolución judicial, y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública.

CONFIDENCIALIDAD y Datos Personales

SANCIONES PENALES (art. 32 incorpora art. 157 bis en el CPA.):

Será reprimido con la pena de prisión de un mes a dos años el que:

I. a sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere a un banco de datos personales;

II. revelare a otro información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley.

CONFIDENCIALIDAD y Datos Personales

ACCION DE HÁBEAS DATA (art. 33 - art. 43 C.N)

La acción de protección de los datos personales o de hábeas data procederá:

a) para tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos.

b) en los casos en que se presuma la falsedad, inexactitud, desactualización de la información, o el tratamiento de datos cuyo registro se encuentra prohibido, para exigir su rectificación, supresión, confidencialidad o actualización.

CONFIDENCIALIDAD y Datos Personales

El **Reglamento General de Protección de Datos (GDPR)** europeo es una serie de reglas y requerimientos dirigidos a proteger los datos personales en manos de empresas y organizaciones para ciudadanos europeos.

Armoniza las leyes de protección de datos personales de los 28 países de la UE.

Rige desde el 25 de Mayo de 2018, y reemplaza la Directiva Europea 95/46/CE sobre el mismo tema.

CONFIDENCIALIDAD y Datos Personales

Principales puntos:

1. Aplicable si hacen tratamiento de datos de europeos.
2. Privacy by Design.
3. Análisis de impacto en el tratamiento para la privacidad.
4. Deber de información mas riguroso.
5. Consentimiento inequívoco positivo en todos los casos (datos sensibles además debe ser expreso).
6. Mayores facilidades para ejercer derechos tradicionales de PDP al que se agregan el “Derecho al Olvido” y la Portabilidad.

(SIGUE)

CONFIDENCIALIDAD y Datos Personales

7. Actitud proactiva en sistemas de seguridad.
8. Obligación de designar *Delegado de Protección de Datos Personales* en algunos casos.
9. Reporte de incidentes de seguridad a las agencias locales con hasta 72hs de plazo.
10. Multas mucho mas severas.
11. Las legislaciones no europeas deberán readecuarse (aunque fuesen adecuadas para la Directiva 95/46/CE, incluida la Argentina).

CONFIDENCIALIDAD y Datos Personales

The EU - U.S. Privacy Shield

Desde 1998, el acuerdo de Puerto Seguro había permitido la transferencia de datos a empresas tecnológicas norteamericanas con presencia en Europa, siempre y cuando cumpliesen con una serie de principios de privacidad.

En 2011, Max Schrems (un estudiante austriaco) llevó a Facebook, Apple, Microsoft, Skype y Yahoo! ante los tribunales europeos acusándolos de traspasar los datos de los usuarios a la Agencia de Seguridad Nacional de los Estados Unidos.

El Tribunal falló a su favor, mostrando las limitaciones de Safe Harbour con la consecuente necesidad de un nuevo acuerdo.

CONFIDENCIALIDAD y Datos Personales

The EU - U.S. Privacy Shield

El TJUE le reprocha a la Comisión Europea que **no** llevara a cabo su obligación de **comprobar si Estados Unidos garantizaba un nivel de protección** de los derechos **"sustancialmente equivalente"** al asegurado en la Unión Europea.

Y **a Estados Unidos que su sistema de protección de datos no está a la altura de lo que el Tribunal europeo considera** necesario para proteger la privacidad de los ciudadanos europeos.

CONFIDENCIALIDAD y Datos Personales

The EU - U.S.
Privacy Shield

El **EU-US Privacy Shield es la normativa que reemplazó a la cuestionada Safe Harbour** que permite la transferencia de datos personales desde la UE hacia los Estados Unidos por parte de organizaciones o empresas que **han sido certificadas por el gobierno norteamericano**.

Solo aplica a empresas reguladas por la Federal Trade Comission (sector comercial), y no, por ejemplo a instituciones financieras o de telecomunicaciones.

CONFIDENCIALIDAD y Datos Personales

The EU - U.S. Privacy Shield

Aquellas organizaciones norteamericanas que vayan a realizar tratamiento de datos de ciudadanos europeos **deberán certificarse ante el Departamento de Comercio de EEUU, y comprometerse públicamente a cumplir con los requerimientos establecidos por el marco regulatorio del Privacy Shield**. https://www.privacyshield.gov/EU-US-Framework

Se publica un listado de empresas certificadas en www.privacyshield.gov/list

CONFIDENCIALIDAD y Datos Personales

The EU - U.S.
Privacy Shield

MARCO REGULATORIO

- Las empresas que quieran importar datos personales desde Europa estarán **obligadas a colaborar con las autoridades europeas de protección de datos personales y a publicar reglas específicas sobre cómo tratan los datos que recopilan**

- **Acceso limitado a las autoridades estadounidenses a los datos personales procedentes de Europa** cuando sea imprescindible, y se realizará con todas las garantías

CONFIDENCIALIDAD y Datos Personales

The EU - U.S. Privacy Shield

- Los **ciudadanos de la UE podrán dirigirse no sólo a las empresas concretas, sino también a las autoridades nacionales de protección de datos** para garantizar que los reclamos no resueltos se investiguen y resuelvan.

- **Creación de la figura de un mediador estadounidense** que se encargará de recibir, tramitar y dar seguimiento a las denuncias y consultas de los usuarios.

CONFIDENCIALIDAD y Datos Personales

DATOS PERSONALES EN LA RELACIÓN ACADÉMICA:

a) La institución debe **tomar recaudos de seguridad de sus bases de datos de alumnos y profesores**.
b) La institución debe **establecer políticas de privacidad efectivas, y designar un delegado de protección de datos personales** a donde los titulares puedan dirigirse para ejercer sus derechos de acceso, rectificación, actualización, bloqueo o supresión de datos.
c) Las **calificaciones y datos de desempeño académico deben ser almacenados en condiciones de seguridad** e informados de modo personal e individual al interesado.
d) Deben **inscribir sus bases** de datos en la Dirección Nacional de Protección de Datos Personales (AAIP).

DERECHO A LA IMAGEN

DERECHO A LA IMAGEN

¿Qué es la imagen?

Representación de algo o alguien por cualquier medio

DERECHO A LA IMAGEN

¿Qué es el derecho a la imagen?

Una persona puede impedir que por cualquier forma se capte, reproduzca, difunda o publique una representación de nuestra persona (nuestra imagen) de un modo que permita su identificación.

- Registros visuales
- Registros auditivos (la voz de una persona).

DERECHO A LA IMAGEN

Ejercicio del Derecho

Ejercicio positivo: autorizar — no puede presumirse (interpretación restrictiva)

Ejercicio negativo: impedir — admite el arrepentimiento

Principio general: La mera reproducción, difusión, divulgación o comercialización de la imagen –fuera de los casos permitidos- constituye iure et de iure un atentado al derecho.

DERECHO A LA IMAGEN

Contenido extra patrimonial

- Relación con el Derecho al Honor y la Dignidad
- ¿Puede ser lesionado el derecho a la imagen sin que haya sido atacada la intimidad?

DERECHO A LA IMAGEN

Sistema anterior al C.C.y C.

- Ley Nº 11.723 – Artículo 31 (Primera parte) : El retrato fotográfico de una persona **no puede ser puesto en el comercio sin el consentimiento expreso** de la persona misma y muerta ésta, de su cónyuge e hijos o descendientes directos de éstos, o en su defecto, del padre o de la madre. Faltando el cónyuge, los hijos, el padre o la madre, o los descendientes directos de los hijos, la publicación es libre.

- La persona que haya dado su **consentimiento puede revocarlo** resarciendo daños y perjuicios.

- Plazo **20 años desde la primer publicación** (Artículo 34). Luego es libre.

DERECHO A LA IMAGEN

Sistema anterior al C.C.y C.

- Excepción:

Ley 11.723 - Artículo 31 (segunda parte): Es **libre** la publicación del retrato cuando se relacione con **fines científicos, didácticos y en general culturales, o** con hechos o acontecimientos de **interés público o que se hubieran desarrollado en público**.

DERECHO A LA IMAGEN

Sistema actual del C.C.y C.

Art. 53.- Derecho a la imagen. Para captar o reproducir la imagen o la voz de una persona, de cualquier modo que se haga, es necesario su consentimiento, excepto en los siguientes casos:

- que la persona participe en **actos públicos**;
- que exista un i**nterés científico, cultural o educacional prioritario**, y se tomen las precauciones suficientes para evitar un daño innecesario;
- que se trate del **ejercicio regular del derecho de informar** sobre acontecimientos de interés general.

Personas fallecidas: herederos o el designado por en testamento.
Si hay desacuerdo entre herederos de un mismo grado, resuelve el juez.

Pasados 20 años desde la muerte, la reproducción no ofensiva **es libre**.

DERECHO A LA IMAGEN

Sistema actual del C.C.y C.

Reemplaza la “puesta en comercio” por “captación” y “reproducción” por cualquier medio, no lo limita sólo al retrato fotográfico .

El consentimiento para el uso de la imagen o voz no requiere que sea expreso.

No es necesario el consentimiento:

a. que la persona participe en actos públicos
b. que exista un interés científico, cultural o educacional prioritario, y se tomen las precauciones suficientes para evitar un daño innecesario
c. que se trate del ejercicio regular del derecho de informar sobre acontecimientos de interés general.

DERECHO A LA IMAGEN

Jurisprudencia

Fallos S.C.J.N.:

- Rodriguez María Belén c/ Google (28/10/2014)
- Gimbutas Carolina Valeria c/ Google (12/09/2017)

Hechos:

- En ambos casos las modelos estuvieron vinculadas a sitios de pornografía y/o prostitución.
- Demandaron a Google, solicitando la eliminación de sus datos personales e imágenes del motor de búsqueda, reclamando además resarcimiento de los daños y perjuicios.

DERECHO A LA IMAGEN

Jurisprudencia

DERECHOS EN PUGNA

Derechos a la libertad de expresión y de información

Derechos al honor, la intimidad y a la imagen

DERECHO A LA IMAGEN

Jurisprudencia

En ambos casos, la CSJN estimó que los proveedores de servicios de Internet ("ISP") **no son responsables por el contenido ilegal de terceros, siempre y cuando el ISP no tuviera conocimiento de la existencia del contenido o si el ISP conociera la existencia del contenido y actuara con prontitud para quitarlo y/o restringir su acceso**.

El dictamen indicó que los ISP todavía tienen la **responsabilidad de eliminar el contenido "manifiestamente ofensivo"** como la pornografía infantil, la incitación a la violencia, y las declaraciones y observaciones difamatorias.

DERECHO A LA IMAGEN

Jurisprudencia

ARGUMENTOS CENTRALES

Responsabilidad subjetiva: Los buscadores no tienen una obligación de monitorear los contenidos que se suben los responsables de páginas web.

Actúan como meros intermediarios: son, en principio, irresponsables por los contenidos que no han creado. Pueden llegar a responder por culpa ante un contenido que le es ajeno, a partir del momento del efectivo conocimiento del contenido ilícito, al no procurar el bloqueo del mismo.

DERECHO A LA IMAGEN

Jurisprudencia

ARGUMENTOS CENTRALES

Para el **“efectivo conocimiento”** requerido para la responsabilidad subjetiva, en aquellos casos donde el **daño resulte manifiesto y grosero basta la simple notificación privada fehaciente**.

En aquellos casos donde el **contenido dañoso exija un esclarecimiento**, para que el buscador tenga conocimiento acerca de la ilicitud, es **necesaria la notificación judicial o administrativa**.

DERECHO A LA IMAGEN

Jurisprudencia

ARGUMENTOS CENTRALES

Toda restricción, sanción o limitación a la libertad de expresión debe ser interpretada en forma restrictiva, y toda censura previa que sobre ella se ejerza padece una fuerte presunción de inconstitucionalidad.

La pretendida eliminación de vínculos existentes que afectan al nombre, imagen, honor e intimidad de la actora, resulta admisible siempre y cuando **se identifique con precisión cuáles son los enlaces asociados (URL)** a su persona y se compruebe el daño que la vinculación ocasiona.

Cuidando de no afectar a la libre circulación de ideas, mensajes o imágenes, y con ello, a la garantía constitucional de **la libertad de expresión.**

DERECHO A LA IMAGEN

Jurisprudencia

ARGUMENTOS CENTRALES

Respecto de los "**thumbnails**", en Gimbutas, la CSJN dijo que constituyen una herramienta para acceder a las imágenes contenidas en páginas de terceros, con el fin de **informar al usuario el sitio web en el que se encuentra la imagen original**.

Que **no difiere de la función de enlace que realiza un "link" de texto** a otro sitio web.

DERECHO A LA IMAGEN

Proyecto de ley Pinedo-Felner

Iniciativa impulsada por dos proyectos de ley: el S-1865/15, de la senadora Liliana Fellner, y el S- 2/16, del senador Federico Pinedo.

Eliminaba la posibilidad de notificar las violaciones al derecho de imagen e infracciones a derechos de autor por medios privados, pero fehacientes, como la carta documento, el telegrama o un simple reclamo administrativo.

Obligando a **iniciar una acción judicial por cada infracción que se comete y a notificar al intermediario de internet por la vía judicial** (cédula de notificación u oficio).

DERECHO A LA IMAGEN

Proyecto de ley Pinedo-Felner

Cuestionamiento: los ISP no son responsables por los contenidos generados por terceros, excepto cuando hayan sido **intimados por orden judicial a bloquear o eliminar un enlace específico publicado.**

Las cámaras, representantes de la industria de los derechos de autor, pedían **utilizar el sistema de notificación (Notice and Take Down/Stay Down)** implementado en Estados Unidos bajo la Digital Millennium Copyright Act (DMCA) para sacar contenidos de la web.

Argumentaron que la orden judicial previa crearía "*un sistema inaccesible, engorroso e ineficiente, ya que es imposible realizar una acción judicial por cada subida ilegal de contenidos que ocasionan daños irreversibles*"

DERECHO A LA IMAGEN

Proyecto de ley Pinedo-Felner

Obtuvo media sanción en el Senado a pesar de ser fuertemente resistida por parte de la industria del derecho de autor (CAL, CADRA, CAP, CAPIF y SAVA, entre otras instituciones).

El día 8 de Noviembre, debido en gran parte, a las fuertes resistencias, **el oficialismo expresó el compromiso de su bloque de dejar "caer" el proyecto.**

Por otra parte, quedó el compromiso de convocar a la totalidad de las instituciones presentes, a partir del próximo año, para evaluar la necesidad de una nueva legislación.

CASOS EN EL AMBITO ACADEMICO

- Marketing Digital
- Grabación de clases
- Exhibición en Página Web Institucional
- Canales de YouTube
- Clases en línea

ESTRATEGIA A ADOPTAR

Gestionar la **autorización expresa de alumnos y profesores** mediante convenios de uso de imagen, donde se establezcan claramente los usos autorizados, la finalidad, los límites y alcances.

MUCHAS GRACIAS

Ab. Federico Andreucci
fandreucci@jus.gob.ar

Créditos: (1) todas las imágenes fueron obtenidas de https://www.kisspng.com/, con licencia de libre uso personal y académico.
(2) todos los cuadros estadísticos fueron obtenidos de https://www.statista.com/

Ministerio de Justicia y Derechos Humanos

Presidencia de la Nación