PROTECCIÓ DE DADES I ALTRES

Jornada de Seguretat Informàtica i protecció de dades a les Policies Locals

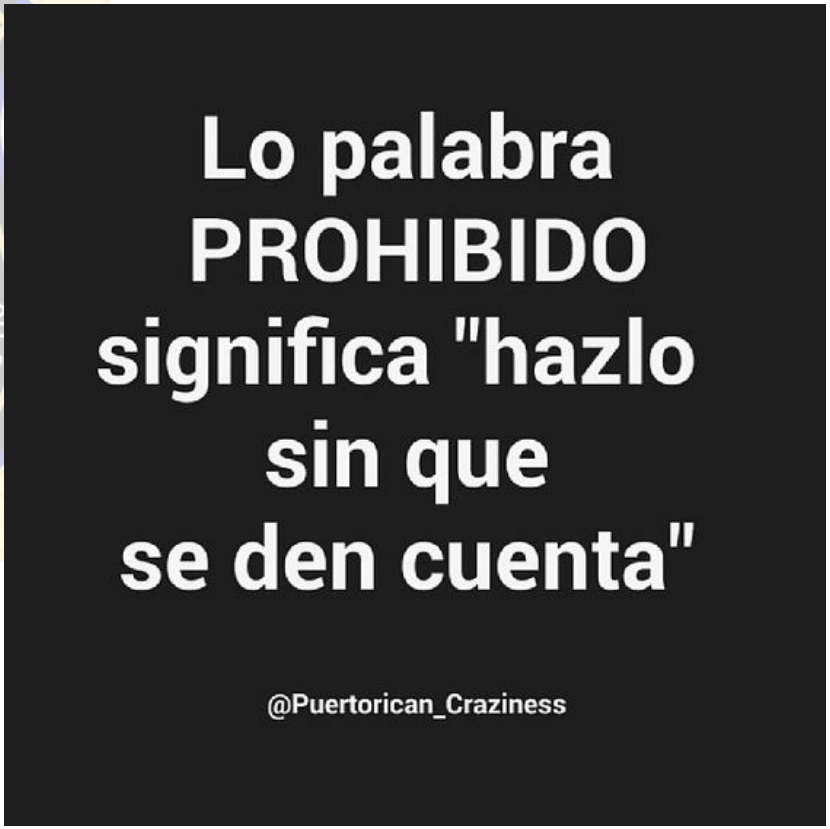
(Seu Federació Catalana de Municipis)
16 de Maig de 2018

josep Jover i Padrò

“...i altres”

-Auditories Econòmiques
-Auditories LOPD
-Auditories LSSI
-Auditories Video
-Auditories Transparència
-Compliance
-Intervenció Pública
-Auditories ISO 26000
-Auditories ISO 27000
-Auditories RSC

Como que no puedo con ellos, los prohibo y... los peritos acaban siendo los gestores de lo prohibido



El tema de las nuevas tecnologias, se ha penalizado, han militarizado la red y la han abierto a los intereses de las grandes empresas

- El Terrorismo tiene las espaldas muy anchas
- El caballero solitario en la red, es ahora un delincuente
- La Red es la histeria de los estados y las oligarquias
- La nueva manera... primero las leyes... luego los tratados

Para retomar el poder, el legislador ha hecho dos cosas

- **Poner en marcha la «Compliance», nuevo negocio de la auditoras**
- **Penalizar y re-penalizar actitudes, costumbres y procedimientos de los nativos digitales**
- **Crear normativa penal en blanco** *contienen la pena pero no consignan íntegramente los elementos específicos del supuesto de hecho, puesto que el legislador se remite a otras disposiciones legales del mismo o inferior rango*
- **Al revés de lo que se ve en el mundo del Derecho, el tema de proteccion de datos ha pasado del administrativo al penal, de lo particular a lo global**
- **Vemos con sarcasmo que los delitos tecnológicos creados para los hackers y las empresas… afectan también a las instituciones públicas… sin la atenuante de la compliance**

Modificar y modificar el Código Penal y dictar normas de guerra

- Y todo por la Adaptación de la estructura a la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas
- y la Directiva 2013/40/UE del Parlamento Europeo y del Consejo de 12 de agosto de 2013 relativa a los ataques contra los sistemas de información
- y a la Publicada la Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica el Código Penal que se acumulaba a la LO 15/2010 de modificacion del Código Penal
- Reglamento (UE) n.º 910/2014 sobre identificación electrónica y servicios de confianza (eIDAS)
- Directiva (UE) 2016/1148, sobre ciberseguridad en vigor desde el 10 de Agosto de 2016

Y es que puede haber además un delito continuado Art.74

1. No obstante lo dispuesto en el artículo anterior, el que, en ejecución de un plan preconcebido o aprovechando idéntica ocasión, realice una pluralidad de acciones u omisiones que ofendan a uno o varios sujetos e infrinjan el mismo precepto penal o preceptos de igual o semejante naturaleza, será castigado como autor de un delito o falta continuados con la pena señalada para la infracción más grave, que se impondrá en su mitad superior, pudiendo llegar hasta la mitad inferior de la pena superior en grado.

2. Si se tratare de infracciones contra el patrimonio, se impondrá la pena teniendo en cuenta el perjuicio total causado. En estas infracciones el Juez o Tribunal impondrá, motivadamente, la pena superior en uno o dos grados, en la extensión que estime conveniente, si el hecho revistiere notoria gravedad y hubiere perjudicado a una generalidad de personas.

O un solo hecho pueden ser a la vez varios delitos Art. 77

1. Lo dispuesto en los dos artículos anteriores no es aplicable en el caso de que un solo hecho constituya dos o más delitos, o cuando uno de ellos sea medio necesario para cometer el otro.

2. En el primer caso, se aplicará en su mitad superior la pena prevista para la infracción más grave, sin que pueda exceder de la que represente la suma de las que correspondería aplicar si se penaran separadamente las infracciones. Cuando la pena así computada exceda de este límite, se sancionarán las infracciones por separado.

3. En el segundo, se impondrá una pena superior a la que habría correspondido, en el caso concreto, por la infracción más grave, y que no podrá exceder de la suma de las penas concretas que hubieran sido impuestas separadamente por cada uno de los delitos. Dentro de estos límites, el juez o tribunal individualizará la pena conforme a los criterios expresados en el artículo 66. En todo caso, la pena impuesta no podrá exceder del límite de duración previsto en el artículo anterior.

• Datos personales y empresariales Codigo Penal Art. 197

ASPERTIC

1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones (*metadatos inclusive*) o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación (*wifi-bluetooth*), será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público *(Axesor*) o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda (*solo acceder*) por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

3. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos (*gestores¡*) o hechos descubiertos o las imágenes captadas (*a medios*) a que se refieren los números anteriores.
Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.

4. Los hechos descritos en los apartados 1 y 2 de este artículo serán castigados con una pena de prisión de tres a cinco años cuando:

a) Se cometan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros; o

b) se lleven a cabo mediante la utilización no autorizada de datos personales de la víctima.

Si los datos reservados se hubieran difundido, cedido o revelado a terceros, se impondrán las penas en su mitad superior.

5. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o una persona con discapacidad necesitada de especial protección, se impondrán las penas previstas en su mitad superior.

6. Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado anterior, la pena a imponer será la de prisión de cuatro a siete años.
7. Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona (*mira la foto que nos hicimos de vacaciones…*).
La pena se impondrá en su mitad superior cuando los hechos hubieran sido cometidos por el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, aun sin convivencia, la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección, o los hechos se hubieran cometido con una finalidad lucrativa.

Datos personales y empresariales Código Penal art. 197 bis

1. El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda (*sólo entrara la wifi*) o facilite a otro el acceso al conjunto o una parte de un ¡¡sistema de información¡¡ (*no hace falta datos personales dentro*) o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.
2. El que mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses.

Datos personales y empresariales Código Penal Art. 197 ter

Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe *(se baje de internet)* o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del artículo 197 o el artículo 197 bis:

a) un programa informático, concebido o adaptado principalmente para cometer dichos delitos; o

b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información.

Datos personales y empresariales Código Penal Art. 197 ter

Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe *(se baje de internet)* o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del artículo 197 o el artículo 197 bis:

a) un programa informático, concebido o adaptado principalmente para cometer dichos delitos; o

b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información.

Datos personales y empresariales Código Penal Art. 197 quarter y quinquies

ASPERTIC

Artículo 197 quater
Si los hechos descritos en este Capítulo se hubieran cometido en el seno de una organización o grupo criminal, se aplicarán respectivamente las penas superiores en grado.

Artículo 197 quinquies
Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en los artículos 197, 197 bis y 197 ter, se le impondrá la pena de multa de seis meses a dos años. Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33.

Código Penal Art. 198

La autoridad o funcionario público que, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior, será castigado con las penas respectivamente previstas en el mismo, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años.

Datos personales y empresariales Código Penal Arts. 199

1. El que revelare secretos ajenos, (*cualquier de cualquiera*) de los que tenga conocimiento por razón de su oficio o sus relaciones laborales, será castigado con la pena de prisión de uno a tres años y multa de seis a doce meses (*periodistas y sus informadores??*).
2. El profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años.

Datos personales y empresariales Código Penal Arts. 200 y 201

ASPERTIC

Artículo 200

Lo dispuesto en este capítulo será aplicable al que descubriere, revelare o cediere datos reservados de personas jurídicas, sin el consentimiento de sus representantes, salvo lo dispuesto en otros preceptos de este Código.

Artículo 201

1. Para proceder por los delitos previstos en este Capítulo será necesaria denuncia de la persona agraviada o de su representante legal. Cuando aquélla sea menor de edad, persona con discapacidad necesitada de especial protección o una persona desvalida, también podrá denunciar el Ministerio Fiscal.

PERO LO QUE LES ACABO DE EXPLICAR...
¡ES UN FRAUDE!

• UNA NUEVA REALIDAD

saben mucho de nosotros?... pues “sólo” el gestor de preferencias de facebook sabe:

Localización física, Edad, Generación, Género, Idioma, Nivel educativo, Área de estudios, Escuela, Afinidad étnica, Renta y patrimonio, Propiedad y tipo de vivienda, Valor de la vivienda, Tamaño de la vivienda, Metros cuadrados de la vivienda, Año en que la vivienda fue construida, segunda vivienda, Composición del hogar, Usuarios en nuevas relaciones, Si tiene un aniversario el próximo mes, Si está lejos de su familia o ciudad natal, Aniversario de amigos, comprometidos, mudados recientemente o de cumpleaños, Usuarios en relaciones a larga distancia, Usuarios con nuevos trabajos, Usuarios recién comprometidos, Usuarios reciéncasados.

• UNA NUEVA REALIDAD

Usuarios recién mudados, Usuarios con cumpleaños cercanos, Padres, Padres en espera de un bebé, Madres, divididas por “tipo” (deportistas, de moda, etc.), Si son propensos a participar en la política, Conservadores y liberales, Estado de relación personal, Empleador, Industria, Título professional, Tipo de oficina, Intereses, Dueños de motocicletas y coches, Si planea comprar un auto (qué tipo, marca y cuándo), Si compró piezas o accesorios de autos recientemente, Si es propenso a necesitar piezas o servicios de automóviles, Estilo y marca de auto que maneja, Año de compra del auto, Edad del auto, Cuánto dinero podría gastar en su próximo auto, Dónde es probable que el usuario compre otro coche, Cuántos empleados tiene su compañía, Dueños de pequeñas empresas, Usuarios que trabajan en gerencia o son ejecutivos, Si ha donado a la caridad (divididos por tipo), Sistema operativo, Si juega en Facebook, Dueños de una consola de videojuegos, Creadores de eventos en Facebook, Si ha realizado pagos en Facebook, Si ha gastado más del promedio en Facebook, Administradores de páginas de Facebook, Si recientemente subió fotos a Facebook (y de quién, aunque no lo diga -programa de reconocimiento facial)

• UNA NUEVA REALIDAD

Navegador de internet, Servicio de mail, segundo mail, Adoptadores tempranos o tardíos de tecnología, Expatriados (divididos por país del que provienen), Si pertenece a una cooperativa de crédito, banco nacional o regional, Inversores (y tipo de inversión), Número de líneas de crédito, Si tiene tarjetas de crédito activas, Tipo de tarjeta de crédito, Usuarios de tarjeta de débito, Si mantiene un saldo en su tarjeta de crédito, Usuarios que escuchan la radio, Preferencia en programas de televisión, Usuarios de un dispositivo móvil (divididos por marca), Tipo de conexión a internet geolocalizada, Usuarios que adquirieron recientemente un dispositivo móvil, Usuarios que acceden a internet por un dispositivo móvil, Usuarios que usan cupones, Tipo de ropa que usan en el hogar, Momento del año en que hace más compras, Compradores asiduos de cerveza, vino o licores, Usuarios que compran comestibles (y qué tipo), Usuarios que compran productos de belleza, Usuarios que compran medicamentos, Usuarios que gastan dinero en productos para el hogar, Usuarios que gastan dinero en productos para niños o mascotas, Usuarios que compran en línia, Tipo de restaurantes que frecuenta, Tipo de tienda en la que compra. Usuarios “receptivos” a las ofertas, Cuánto tiempo vivió en su casa, Usuarios propensos a mudarse pronto

• UNA NUEVA REALIDAD

Interesados en los Juegos Olímpicos, fútbol, cricket o Ramadán, Si viaja con frecuencia (trabajo o placer), Si se desplaza para trabajar, Tipo de vacaciones a las que suele ir, Si recién volvió de un viaje, Si usó una app de viajes, Si participa en un tiempo compartido

+ GEOLOCALIZACION DE CADA CONEXION, PUDIENDO IDENTIFICAR A OTROS GEOLOCALIZADOS CONEXOS EN ESE MOMENTO,
+ PROGRAMA DE RECONOCIMIENTO FACIAL (CON QUIEN ME HAGO LA FOTO), GEOGRAFICO (IDENTIFICACION DE LA MONTAÑA/EDIFICIO QUE TENGO DETRAS)
+ PROGRAMA DE INTERPRETACION DE CARACTER (SI ESTOY TRISTE O ALEGRE)
+ OPCION SEXUAL AL DETALLE
+ EVOLUCION DE MI PERSONALIDAD, SALUD E INTERESES (ANALISIS DOCUMENTAL)

ESO ES LA BASE DEL **BIG DATA**

Introducción

NOS VIENE IMPUESTA POR LAS LEYES

DIRECTIVA COMUNITARIA, y proximamente Reglamento COMUNITARIO (afectacion a todos los países UE)
OTRAS DIRECTIVAS COMUNITARIAS ESPECIFICAS (Telecomunicaciones, ciberseguridad, ...)
LEY ORGANICA 15/99 LOPD
OTRAS NORMAS ESPECIFICAS ORGANICAS (CODIGO PENAL, LEY DE LA FUNCION PUBLICA, CODIGO CIVIL) ESTATUTOS
REGLAMENTO DE SEGURIDAD (2007)
REGLAMENTOS SECTORIALES Y OTRAS NORMAS DE APLICACIÓN DE CARÁCTER NO ORGÁNICO
INSTRUCCIONES DE LA AGPD Y DE LAS AGENCIAS AUTONÓMICAS
CODIGOS TIPO INSCRITOS
CONSULTAS A LA APD
AUDITORIA LOPD
DOCUMENTO DE SEGURIDAD

CONFORME VAMOS BAJANDO AL DETALLE LAS NORMAS SE VAN CONCRETANDO

Introducción

Y SOBRETODO POR LAS SENTENCIAS….

A) Sentencia de 6 de octubre de 2015, asunto C-362/14 (*conocida como Safe Harbour),* donde se declara POR SEGUNDA VEZ, inválida la Decisión de la Comisión que declaró que Estados Unidos garantiza un nivel adecuado de protección de los datos personales transferidos. La anterior Sentencia es la de 30 de Mayo de 2006, asuntos C-317/04 y C-318/04.

B) Sentencia de 1 de octubre de 2015, asunto C-230/14, donde se declara que la normativa de un Estado, en protección de datos, puede aplicarse a una sociedad extranjera que realice en ese estado una actividad real y efectiva mediante una instalación estable. Habla también esta sentencia de la necesaria diligencia en la cooperación entre autoridades de control de diversos estados.

C) Sentencia de 1 de octubre de 2015, asunto C-201/14, donde se declara que las personas cuyos datos personales son objeto de transmisión y tratamiento entre dos administraciones públicas, deben ser informadas de ello previamente.

Introducción

Y SOBRETODO POR LAS DIRECTIVAS

A) Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave.

B) Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

C) Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) no 2006/2004 sobre la cooperación en materia de protección de los consumidores.

Introducción

Y SOBRETODO POR LAS DIRECTIVAS

D) Directiva 2006/24/CE, del Parlamento Europeo y del Consejo de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.

E) Directiva 2004/82/CE, del Consejo de 29 de abril de 2004, sobre la obligación de los transportistas de comunicar los datos de las personas transportadas.

F) Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre privacidad y las comunicaciones electrónicas).

G) Directiva 2002/22/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas (Directiva servicio universal).

H) Directiva 2002/21/CE, del parlamento Europeo y del Consejo de 29 de abril de 2004, sobre la obligación de los transportistas de comunicar los datos de las personas transportadas.

Introducción

Y SOBRETODO POR LAS DIRECTIVAS

I) Directiva 2002/20/CE, del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a la autorización de redes y servicios de comunicaciones electrónicas (Directiva de autorización).

J) Directiva 2002/19/CE, del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión (Directiva de acceso).

K) Directiva 2000/31/CE, del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico).

L) Directiva 1999/93/CE, del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.

M) Directiva 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones. (Derogada por la Directiva 2002/58/CE).

El perito informático es como el bikini. Cuando interviene, aparecen los michelines que venian siendo disimulados por la ropa de cada dia, y ya nada es lo mismo.