Trabajo Práctico

Impacto ético, social y legal de las tecnologías de información

Objetivos específicos:

- Conocer normas legales que impactan en sistemas de información y los activos de Tecnología de la Información (TI) que lo soportan
- Identificar factores de riesgo legal en sistemas de información

EJERCICIO 1:

ANÁLISIS DE NORMATIVAS: SECRETO PROFESIONAL VS. DEBER DE CONFIDENCIALIDAD VS. INOPONIBILIDAD SECRETO PROFESIONAL.

Referencia 1: Código de Etica para Profesionales de las Ciencias Económicas de Salta (Res. Gral. Nº 855/94)

SECRETO PROFESIONAL
Artículo 20.- La relación entre profesionales y clientes debe desarrollarse dentro de la más absoluta reserva y confianza. No deben divulgar asunto alguno sin la autorización expresa del cliente, ni utilizar en su favor o en el de terceros el conocimiento íntimo de los negocios del cliente, adquirido como resultado de su labor profesional.
Artículo 21.- Están relevados de su obligación de guardar secreto profesional cuando imprescindiblemente deban revelar sus conocimientos para su defensa personal, en la medida en que la información que proporcionen sea insustituible o cuando concurra obligación legal.

Referencia 2: Ley de Protección de Datos Personales (Nº 25.326)

Artículo 10. — (Deber de confidencialidad).

1. El responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos. Tal obligación subsistirá aun después de finalizada su relación con el titular del archivo de datos.

2. El obligado podrá ser relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública.

Referencia 3: Ley de Prevención de Lavado de Dinero (Nº 26.683)

Artículo 15. — Sustitúyese el artículo 20 de la ley 25.246 y sus modificatorias, por el siguiente:

Artículo 20: Están obligados a informar a la Unidad de Información Financiera (UIF), en los términos del artículo 21 de la presente ley:

……

17. Los profesionales matriculados cuyas actividades estén reguladas por los consejos profesionales de ciencias económicas;

Artículo 14. — Sustitúyese el artículo 14 de la ley 25.246 y sus modificatorias, por el siguiente:

Artículo 14: La Unidad de Información Financiera (UIF) estará facultada para:

1. Solicitar informes, documentos, antecedentes y todo otro elemento que estime útil para el cumplimiento de sus funciones, a cualquier organismo público y a personas físicas o jurídicas, públicas o privadas, todos los cuales estarán obligados a proporcionarlos dentro del término que se les fije, bajo apercibimiento de ley.

En el marco del análisis de un reporte de operación sospechosa los sujetos contemplados en el artículo 20 no podrán oponer a la Unidad de Información Financiera (UIF) el secreto bancario, fiscal, bursátil o profesional, ni los compromisos legales o contractuales de confidencialidad.

Se pide:

- Leer las tres referencias normativas.
- Analizar el tema: secreto profesional en base a la siguiente hipótesis:
  ¿Ud. futuro profesional de ciencias económicas cómo cumpliría estas tres referencias normativas que impactan en su profesión ante una situación donde debe reportar una operación sospechosa de un cliente suyo?

EJERCICIO 2:

LA PROTECCIÓN DE DATOS PERSONALES Y DE LA PRIVACIDAD EN TIEMPOS DE PANDEMIA

Fuente: http://www.saij.gob.ar/maria-florencia-bossi-proteccion-datos-personales-privacidad-tiempos-pandemia-dacf200038-2020-03-24/123456789-0abc-defg8300-02fcanirtcod?&o=3&f=Total%7CFecha%7CEstado%20de%20Vigencia%5B5%2C1%5D%7CTema%5B5%2C1%5D%7COrganismo%5B5%2C1%5D%7CAutor%5B5%2C1%5D%7CJurisdicci%F3n%5B5%2C1%5D%7CTribunal%5B5%2C1%5D%7CPublicaci%F3n%5B5%2C1%5D%7CColecci%F3n%20tem%E1tica%5B5%2C1%5D%7CTipo%20de%20Documento/Doctrina&t=5. Fecha Consulta: 30-3-21

El Coronavirus (COVID-19), cuyos primeros casos fueron registrados en la ciudad china de Wuhan, en noviembre de 2019, se ha propagado a un ritmo vertiginoso en gran parte del mundo. Como consecuencia de ello, en marzo de 2020, la enfermedad fue considerada "pandemia" por la Organización Mundial de la Salud.
Más allá de la amenaza sanitaria, la pandemia trajo consigo toda una serie de implicancias jurídicas en materia de protección de datos personales, sobre las que vale la pena reflexionar.
En tal sentido, el Comité Ejecutivo de la Asamblea Global de Privacidad emitió un documento con pautas sobre la materia, con el objeto de colaborar en el desafío que implica abordar el avance del nuevo coronavirus y el intercambio de datos personales.

En Europa, diferentes autoridades se han referido a la problemática de la protección de los datos personales en el contexto de la pandemia, y el Comité Europeo de Protección de datos emitió una declaración en la que destaca que la regulación vigente - y en particular el nuevo reglamento europeo - no impiden tomar medidas en la lucha contra el flagelo del coronavirus. Sin embargo, en el documento se advierte que quienes traten datos personales deben asegurar su protección, aún en estas circunstancias de excepción.

Italia, uno de los países más golpeados por la enfermedad, aprobó una legislación de emergencia que obliga a toda persona que haya estado recientemente en una zona de riesgo, a notificar de ello a las autoridades sanitarias.
En el caso de España, otro de los países más perjudicados por el virus, la Agencia de Protección de Datos de dicho país ha publicado un informe en el que analiza el tratamiento de datos personales en relación con la crisis epidemiológica y un listado de "Preguntas Frecuentes" sobre el Coronavirus, centradas en el tratamiento de datos en el ámbito laboral.
En lo que respecta a los desarrollos tecnológicos al servicio de la emergencia, varios de los países afectados han implementado sistemas que permiten hacer un seguimiento de la ubicación de las personas. En China y otros países asiáticos, las medidas han sido aún más rotundas y polémicas. La explicación a ello puede encontrarse en diversos factores, dentro de los cuales pueden mencionarse aquellos de tipo cultural y político. No puede olvidarse que, en muchos de estos países, la protección de datos no se considera un aspecto tan prioritario y los Estados suelen tener una mayor injerencia en la vida y la privacidad de sus ciudadanos.
En el caso de China, país que en un principio ha sido epicentro de la enfermedad, se ha implementado el uso de aplicaciones, inteligencia artificial y otras tecnologías semejantes a fin de mitigar la expansión de la enfermedad.
Uno de los ejemplos más notorios es la implementación de una aplicación móvil que permite obtener información sobre los lugares en los que ha estado cada persona durante los últimos días, valiéndose de los datos recolectados por las torres de telefonía a las que los usuarios conectan sus dispositivos.
En base a ello, se aplicó un sistema de clasificación basado en códigos QR de tres colores, en función de los lugares en donde había estado cada persona y si mostraba síntomas; dependiendo del código asignado, la persona debía quedarse en cuarentena o podía moverse libremente.
En Argentina, la Agencia de Acceso a la Información Pública ha emitido un comunicado en su sitio de Internet, en el cual informa sobre las pautas y las bases de legitimidad para el tratamiento de datos personales en el marco de la pandemia.

Se pide:

- Analizar el articulo
- Mencionar las principales disposiciones relevantes de la ley de protección de datos personales argentina con respecto al tratamiento de datos en el contexto de pandemia

EJERCICIO 3:

PRIMERA DECISIÓN JUDICIAL ARGENTINA SOBRE APROPIACIÓN DE CRIPTOMONEDAS

Fuente: Tomo La Ley 2019-B. Año LXXXIII N° 68. ISSN 0024-1636.

A continuación, se describen los hechos del caso:

El 21 de noviembre de 2018 la sala III de la Cámara Tercera en lo Criminal de la Provincia de Chaco dictó sentencia en el marco de la causa "P., H. M. s/ defraudación informática en concurso real con violación de secretos y de la privacidad", en la cual se dispuso la primera condena por la "apropiación" de criptomonedas en la República Argentina.

Los hechos que motivaron el caso fueron los siguientes:

- Entre los días 14 de diciembre y 16 de diciembre del 2017, el Sr. H. M. P. realizó un ataque informático al exchange "Mercury Cash", mediante el cual logró acceder a los sistemas de la empresa afectada, mediante una técnica de

ataque muy común (se trató de una inyección de SQL en el código de la base de datos del exchange. Esta forma de ataque a sitios web que generalmente usan Java, SQL o PHP consiste en aprovechar fallas en las rutinas de validación de acceso para lograr el acceso a la base de datos de SQL del sitio, y de esa forma acceder a las contraseñas del administrador del sistema. Cabe aclarar que todo acceso no autorizado surge de una falla en el desarrollo de la aplicación o de un error humano. En el primer caso, las vulnerabilidades que permiten una inyección de SQL se originan generalmente en un error en el desarrollo. Por eso muchas empresas que desarrollan software de seguridad implementan un "ciclo de vida" seguro en el desarrollo. Pero es casi imposible llegar a testear todas las opciones posibles antes de lanzar un producto un producto de software. En la práctica la seguridad nunca está 100% garantizada), y tomar su control.

- Ello le permitió cursar transferencias de ether, la criptomoneda asociada a la blockchain de Ethereum, a cuentas que el condenado mantenía en otras plataformas, para luego descargarlas en una billetera de su titularidad y dominio almacenada en un teléfono celular.
- En total el atacante logró transferir fuera del exchange "Mercury Cash" un total de 500 ethers, que a la fecha del hecho delictivo equivalían a la suma de u$s 434.352. A la fecha de diseño del presente práctico: 30/03/2021 equivalen a u$s918.000.
- El atacante fue identificado gracias a las medidas de seguridad informática que mantenía el exchange, que permitió identificar las direcciones IP desde las cuales el atacante ingresó al sistema, así como también gracias a la colaboración entre los exchanges, ya que parte de las primeras direcciones a las cuales se enviaron ethers eran de billeteras de otros exchanges.

Se pide:

- Analizar el caso
- Identificar tipos de delito informático según ley 26.388
- En caso positivo, mencionarlos