TERRITORIES OF TOMORROW
Territoires de Demain
Territorios del Mañana
2021
La Revista anual "Ecosistema de Innovación Abierta y disruptiva",
Áreas temáticas:
Ciencia y Tecnología, Ciudades Inteligentes, Empoderamiento, E-Emprendimiento, Frech Tech Hub, Internet de las Cosas, E-Salud, Big Data,Gobierno Abierto, Gestión del Conocimiento, Desarrollo Sostenible, Telemedicina, M-Salud, IA...
ISSN 2606-2984 - Dépôt légal décembre 2017
Le Magazine annuel «Écosystèmes d'innovation ouverte et disruptive»,
Domaines thématiques:
Science et technologie, Villes intelligentes, Empowerment, E-Entrepreneurship, Hub technologique Frech, Internet des objets, E -Santé, Big Data, Gouvernement Ouvert, Gestion des Connaissances, Développement Durable, Télémédecine, M-Santé, IA...
http://www.territories-of-tomorrow.org/

Tecnoética: hacia un código moral

Santiago F. Parra y Federico A. Carmona
https://uai.edu.ar/

Facultad de Tecnología Informática, Universidad Abierta Interamericana, Buenos Aires, Argentina

Tutora: Mg. Lic. Susana Darin

Resumen: El presente trabajo intenta poner en la agenda académica la necesidad de realizar un análisis profundo y debate sobre los principios de un código ético para los graduados en las carreras de Ingeniería en Sistemas, Ciencias de la Computación, Ingeniería Electrónica y afines. Un juramento hipocrático, como en Ciencias Médicas, de carácter ético que comprometa y oriente a los profesionales en la práctica del ejercicio de la profesión. De esta forma se evitarán situaciones de riesgo que pongan en peligro a los ciudadanos, las organizaciones con y sin fines de lucro y al propio Estado.

Es evidente que en el paradigma de la globalización caracterizado por el auge las economías de plataforma y la economía digital, entre otras, existe una tendencia a la manipulación y uso de datos con fines que ponen en riesgo a los ciudadanos, el sector privado y al propio Estado.

Palabras Clave: Ética, Tecnoética, Uso de Datos, Hacking, Juramento Hipocrático.

Abstract: The present work tries to put on the academic agenda the need to carry out a deep analysis and debate on the principles of an ethical code for graduates in the careers of Systems Engineering, Computer Science, Electronic Engineering and others related. A Hippocratic oath, as in Medical Sciences, of an ethical nature that commits and guides professionals in the practice of the exercise of the profession. In this way, risk situations that endanger citizens, for-profit and non-profit organizations, and the State itself would be avoided.

It is evident that in the paradigm of globalization characterized by the boom of platform economies and the digital economy, among others, there is a tendency to manipulate and use data for purposes that put citizens, the private and public sector and the state itself at risk.

Keywords: Ethics, Technoethics, Data Usage, Hacking, Hippocratic Oath.

Introducción

Este trabajo tiene por objetivo poner en evidencia que en ciertas ocasiones se utilizan los conocimientos (en el campo de la tecnología) con fines que perjudican directa o indirectamente a la sociedad, el sector privado e inclusive al Estado.

El mundo globalizado se encuentra nucleado bajo una gran red denominada internet, la cual nos permite interrelacionarnos pero que a su vez nos deja expuestos a riesgos que antes de 1969[3] no se contemplaban.

Una problemática que surge con la invención del internet y aún continúa es el desconocimiento de las herramientas para protegerse al momento de navegar por los sitios web, redes sociales, entre otras aplicaciones. Además, los usuarios no están completamente conscientes de los riesgos que implica brindar los datos personales a través de internet para el registro en una red social, entidad bancaria o empresa.

A partir de la investigación realizada, se encontraron diferentes propuestas de dos fuentes principales provenientes de JVV Grup y Xataka quienes indican la necesidad de realizar un Juramento Hipocrático para los graduados en el campo de la Ingeniería Electrónica. Este juramento puede ser extensible a Ingeniería en Sistemas Informáticos, Lic. en Sistemas, Analista en Sistemas Informáticos, Ciencia de datos e Ingeniería de Telecomunicaciones, es decir profesiones en las cuales se manipulen datos a gran escala.

El trabajo plantea la siguiente hipótesis: "*la falta de un juramento hipocrático en el área tecnológica implica un riesgo cuando los conocimientos, habilidades y destrezas adquiridas por un profesional no son utilizadas bajo principios éticos y morales*".

A lo largo del escrito se explicarán términos importantes para entender la relevancia de proteger los datos personales y a lo que estamos expuestos cuando se los delegamos a terceros. También se observará cómo es posible que profesionales que trabajan para ciertas empresas renombradas en el mundo de IT en proyectos que financian las mismas para beneficio propio o para la simple investigación, luego utilizan todas las investigaciones y pruebas realizadas para vendérselas a otras empresas o incluso a Países.

[3]Año en donde surge ARPANET, red militar creada por EE. UU durante la guerra fría que en caso de que se realice un ataque ruso se pudiera tener información militar desde cualquier lugar del país.

1. Aclarando conceptos clave

En el presente trabajo partimos de los siguientes conceptos:

La ética es una de las ramas más antiguas de la filosofía dedicada al estudio de la conducta humana, expresada en conceptos como lo correcto y lo incorrecto, lo bueno y lo malo, la virtud, la felicidad y el deber, así como en los sistemas de valores que dichas categorías sostienen. Estudia los valores morales que guían el comportamiento humano en la sociedad, mientras que la moral son las costumbres, normas, tabúes y convenios establecidos por cada sociedad.[1]

La tecnoética surgió como concepto en los años 1970 cuando Bunge[9] consideró que era necesario crear un nuevo concepto de ética que incluya el aspecto tanto científico y tecnológico, también creía correcto que los profesionales que se desarrollaban en los campos mencionados anteriormente se rijan bajo un nuevo código ético que contemple nuevas responsabilidades morales y sociales. La tecnoética implica el estudio de los códigos morales bajo los que se rigen quienes participan en las diversas ramas de la tecnología. [2]. Se estima que el 40% de los ingenieros alrededor del mundo se ven implicados en alguna medida en la producción de armamentos aún cuando gran cantidad de estos realizaron juramentos o promesas ante universidades, iglesias y demás entidades. Se entiende que esto corresponde a la falta de un código moral y ético que regule internacionalmente el accionar de los profesionales y que cuente con un marco jurídico. [4]

Los datos personales engloban toda información propia de una persona y que se relaciona con la misma como es el ejemplo del número del Documento Nacional de Identidad, número de teléfono, información crediticia, imágenes, domicilio, entre otros. Teniendo en cuenta la definición anterior es importante comentar los derechos que tiene cada individuo en cuanto al acceso a la información de sus datos personales ya que no es muy difundida.

Los datos sensibles son todos aquellos que den cuenta de tu origen racial, étnico, opiniones relacionadas con tu libertad de expresión (políticas, por ejemplo), preferencias religiosas, morales, éticas, filosóficas, afiliación sindical e información relacionada con la vida sexual o estado de salud.

2. Derechos que protegen los datos personales

El derecho a la información permite que tengas conocimiento acerca de las bases de datos personales registradas, quienes son sus responsables y el domicilio legal. Esto da paso al ejercicio de los otros derechos que se detallarán a continuación, para obtener esta información se debe ingresar a la página web del Registro Nacional de Bases de Datos Personales (RNBD).

El derecho de acceso te da la posibilidad de conocer si una empresa, entidad, organismo público o profesional tiene en su poder datos de tu persona, donde los obtuvo y con que fin los utiliza. Algunos aspectos para tener en cuenta sobre este derecho: se puede solicitar el acceso de forma gratuita cada seis meses realizando el pedido a la entidad, empresa, organismo o profesional que posea tus datos, podes ver la información en el RNBD. Es recomendable realizar el pedido a través de un medio en el cual puedas obtener una constancia del mismo o una copia del escrito enviado, lo cual facilita que en

[9] Fue un filósofo, epistemólogo y físico fallecido en el año 2020 de nacionalidad argentina.

el caso de que de incumplimiento de la solicitud o exceso del plazo prestablecido (diez días de corrido) se tomen las acciones correspondientes que implican la denuncia ante la Dirección Nacional de Protección de Datos Personales de la Agencia de Acceso a la Información Pública o bien realizar una presentación judicial, acción de Habeas Data[5].[3]

3. Malas prácticas de los profesionales de la tecnología

3.1 Trend Micro

La compañía Trend Micro en el año 2019 informó que sufrió un grave incidente de seguridad. El problema consistió en que un empleado robó y vendió datos de unos 68.000 de sus clientes de consumo. El empleado vendió a terceros datos personales, entre estos se encontraban nombre, números de teléfono y direcciones de correo electrónico. El trabajador obtuvo los datos a partir de una base de datos de soporte técnico. No logró acceder a la información crediticia de los clientes debido a que no figuraban en esa base de datos.

Este hecho tuvo como consecuencia la afección de clientes ya que cuando se comercializaron sus datos comenzaron a recibir llamados de personas que aparentaban ser trabajadores del departamento de soporte de la misma empresa para intentar obtener aún más datos que les permita conseguir un rédito económico de la cuenta de estas personas.

En este suceso ocurrido en noviembre del año pasado podemos observar como es que una persona profesional en ámbito tecnológico (ya que por ello se encontraba en el área de soporte técnico) considerada idónea para el manejo de datos personales puede violar la privacidad de estos y como se viene comentando desde la introducción es en parte de la falta de un código ético rígido. [6]

3.2 United Microelectronics Corporation (UMC)

Dos ingenieros de la empresa taiwanesa UMC fabricante de chips de memoria Micron filtraron la tecnología de su antiguo empleador y utilizaron secretos comerciales en un proyecto de cooperación con un fabricante estatal chino de semiconductores. El supervisor también fue procesado por la participación en el plan.

Si bien se sentenció a los tres empleados de UMC a una pena de entre 4.5 a 6.5 años de prisión por violar la ley de Taiwán sobre secretos comerciales sumado a una multa de 3.37 millones de dólares y a su vez fueron acusados de cargos similares por los fiscales federales de Estados Unidos, se sigue sosteniendo que la falta de moral por parte de los profesionales le lleva a realizar estas “traiciones” a los principios éticos y a empresas para las cuales trabajan. [7]

3.3 Avast

La reconocida empresa de antivirus para dispositivos electrónicos Avast fue objeto de una investigación que expuso que la empresa vende información de los datos personales de los usuarios y que este sería el principal ingreso ya que su descarga es gratuita. Según esta investigación Avast recopila los datos y los vende a través de una empresa

[5] el Habeas Data es un tipo de amparo que permite a toda persona interesada acceder al conocimiento de los datos que consten en una Base de Datos [5].

tercerizada que tiene el nombre de Jumpshot. Estos datos se comercializan a empresas interesadas en la interacción de los usuarios con las páginas web, esto es posible ya que el antivirus registra cada movimiento que se realiza con el mouse o el cursor y cada enlace que se visita. Se estima que Avast tiene alrededor del mundo 435 millones de descargas en diversos dispositivos electrónicos por lo cual la cantidad de datos recopilados es muy grande. Entre las empresas que reciben los servicios de Jumpshot se encuentran IBM, Microsoft, Google, Amazon y Pepsi, aunque las dos primeras mencionadas desmintieron que hayan sido clientes de esta.

Afirman que Avast vende distintos paquetes de datos con diferentes grados de acceso. La empresa se escudó diciendo que la obtención de datos a través de las extensiones web fue una práctica que realizo por seguridad y que ya no lo realiza.

El inconveniente finalizó cuando el senador Wyden afirmó que Avast dejaría de realizar esta recolección de datos, pero dejó claramente establecido que la empresa si había obtenido datos y que le preocupaba que no se eliminaran aquellos que se habían obtenido sin consentimiento ni a dejar de realizar la venta de datos confidenciales.

Nuevamente es totalmente engañoso lo que realiza la empresa Avast y como comercializó datos personales, los cuales como se vio en la sección "Conceptos clave" no puede utilizarlos nadie a quien el propietario de estos no le de acceso. [8]

3.4 Google

La renombrada empresa Google fue acusada de dar en secreto datos personales de usuarios a empresas que realizaban anuncios. Irlanda se encuentra bajo una investigación en la cual tiene como objetivo demostrar que la empresa recopiló información confidencial a través de páginas web ocultas y se las ofreció a los anunciantes. El regulador irlandés está encargado de supervisar la actividad de Google en Europa, puntualmente en este caso se está investigando si la tecnología norteamericana emplea información confidencial de los usuarios, en términos de datos sensibles, como vimos en el primer punto de este escrito, etnia, salud, pensamiento político y demás.

Esta falta a la privacidad de los usuarios fue detectada por Johnny Ryan[6], el cual realizó un seguimiento de sus datos en un sitio de subastas de publicidad y descubrió que Google le había incorporado un rastreador de identificación que alimentaba a compañías externas que iniciaban sesión en una página web oculta. Estas practicas vulneran todo tipo de regulaciones, en este caso detectado en la Unión Europea.

Es preciso realizar una síntesis de lo que se buscó visualizar con los cuatro casos desarrollados anteriormente. Se tuvo que realizar una elección de la cantidad de casos que hay sobre como las empresas violan la privacidad de los usuarios. Se seleccionaron los más emblemáticos y que impliquen a empresas con más renombre para demostrar que muchas empresas, hasta las más renombradas, tienen aspectos que son correctos y nuevamente, se entiende que sucede a raíz de que no existe un código ético que rija el funcionamiento de las empresas tecnológicas y en especial los profesionales que las integran. [9]

---

[6] Responsable de Políticas y Relaciones con la Industria del navegador Brave (modesto navegador, uno de los rivales de Google)

4. Juramento Hipocrático y su aplicación en la tecnología

Es correcto realizar esta analogía en dos aspectos fundamentales, el primero para que se establezca una idea clara sobre como sería una solución a la falta de ética en la tecnología y que se plantea como solución a la hipótesis de este trabajo. Y en segundo lugar para poner un ejemplo de como se deben tratar los datos sensibles, ya que como vimos anteriormente uno de ellos es el estado de salud.

¿Qué es el juramento hipocrático? El juramento hipocrático existe hace más de 2500 años cuando Hipócrates (por eso el nombre del juramento) estableció cuales debían ser las obligaciones de quienes ejercen la medicina. Las acciones legales que se puedan llegar a tomar en caso de que se realice una mala práctica de la medicina se rigen principalmente por estos postulados éticos y morales que entre ellos los principales deberes implican: consagrar la vida propia al servicio de la humanidad, ejercer la profesión con conciencia y dignidad, hacer de la salud y de la vida de los enfermos la primera de sus preocupaciones, considerar a los colegas como hermanos, no utilizar los conocimientos médicos contra las leyes de la humanidad, entre otros. Pero es interesante un punto que establecen que está íntimamente relacionado con el trabajo en desarrollo ya que habla de los datos y da cuenta que aún cuando la persona fallezca no se levanta el carácter reservado de su historia clínica (datos sensibles), esto se entiende como un derecho que está unido a la persona y es inseparable de ella. [10]

Es interesante observar cómo se venera al individuo gracias a los postulados de este juramento e inclusive en la práctica ya que se basan en la ética del documento hipocrático, lo cual les da un rumbo y les inculca la ética desde un principio. Se respetan los datos de las personas en cualquier instancia de sus vidas y por eso se busca demostrar a lo largo de este texto que promover un código similar para el ámbito tecnológico reduciría la mala actuación de ciertos trabajadores en dicha área, que solo ven los datos de las personas como una forma de comercio, y si no se hace foco en esta problemática la privacidad dentro de unos años sería mucho menor de lo que es en la actualidad.

5. Economía de plataforma y su relación con los datos

5.1 Definición de economía de plataforma

La economía de plataforma es aquella que se desempeña a través de plataformas digitales que regulan la oferta y demanda en tiempo real, generalmente a través de dispositivos móviles. Abarca desde productos alimenticios hasta inmobiliarios. Esta tecnología permite que se pueda acceder a las diversas aplicaciones desde cualquier dispositivo que posea internet o una red móvil. [11]

5.2 Relación con los datos

Las empresas BigTech[7] de Silicon Valey[8] guardan datos como capital. Esta economía digital tiene la capacidad de diariamente recopilar, analizar, y utilizar diariamente una gran cantidad de datos. Toda esta información es cotidianamente utilizada a fin de conformar el valor central de la economía de plataformas. Estos datos son un conjunto de rastros que deja cada usuario por actividades personales, sociales, culturales u

[7] Así se las denomina a las empresas más grandes que dominan la industria del IT.
[8] Es un lugar geográfico ubicado en San Francisco, EE. UU, que es el centro donde se encuentran.

empresariales que se realizan en diversas plataformas digitales de la WWW (World Wide Web).

Estados Unidos junto con sus aliados políticos y económicos al tener un fuerte control sobre los posicionamientos en política global quieren lograr que todos los países firmen un régimen de "flujo de datos globales libres". Si se logra este objetivo, se deben regular aún más para que no se realice una mala o interesada utilización de estos.

Esta idea de convertir los datos en un producto de comercio plantea desafíos de veracidad y valor de los datos. Las empresas o entidades que promueven esta práctica de recopilar, analizar, comercializar datos se encuentran enfocadas en producir este "producto" no natural.

Las leyes que se encuentran actualmente acerca de la protección de datos no ponen el foco en la dimensión económica de los mismos. En este tipo de economía las publicidades personalizadas son fundamentales, motivo por el cual los datos de cada usuario son vitales para que se pueda realizar este direccionamiento de anuncios.

A continuación, se verá como ha ido evolucionando la internet a lo largo de los años y un cierto pronóstico para el futuro, es un gráfico que desarrolló el Informe sobre la Economía Digital UNCTAD el año pasado

Fig. 1. Evolución de tráfico a través de Internet a nivel mundial.

Particularmente en Latinoamérica la protección sobre el derecho ciudadano de los datos personales es muy escasa o en algunos casos ni existe. [12]

6. Autores que avalan la idea de un juramento hipocrático

Al realizar una minuciosa investigación se halló que había algunos autores que apoyaban la idea acerca de que crear un juramento hipocrático en el área tecnológica, a continuación, se darán los dos ejemplos que para los autores de este trabajo resultaron de mayor relevancia.

6.1 JVV Grup

Se encontró que la empresa JVV Grup[9] realizó un breve texto en el cual exponía sus ideas de porque es necesario aplicar un juramento hipocrático en el campo de la Ingeniería Electrónica.

La empresa opinó lo siguiente:

> Creemos que los ingenieros debemos tomar consciencia del poder que tiene la tecnología. De no ser así, el uso del *big data* podría convertirse en una actividad perjudicial para la sociedad.
>
> Ya hace tiempo que se está planteando la posibilidad de adoptar un juramento hipocrático para ingeniería, parecido al que se aplica en medicina. El uso ético de la tecnología debe estar presente en nuestro trabajo diario, y es que no podemos ignorar la repercusión que éste tiene en la sociedad. Los ciudadanos se exponen a la tecnología, y deben conocer su uso y qué datos se generan; por ello, los ingenieros debemos respetar ciertos valores. (JVV Grup, 2019, "La necesidad de un juramento hipocrático en el sector de la ingeniería electrónica", párrafo 1 y 2)

6.2 Xataka

Xataka en una publicación que lanzó en su página web realizada por el autor Carlos Prego informaba sobre los motivos por los qué es preciso que se cree el juramento hipocrático en todo el ámbito tecnológico. A continuación, se hará alusión al contenido de esa nota y se citará textualmente cuando se considere necesario.

Se da cuenta que los Ingenieros Informáticos pasan a lo largo de toda su carrera universitaria estudiando materias como las matemáticas, lógica, física, arquitectura de sistemas, programación, entre otras y la cuestión ética y moral pareciera pasar a un segundo plano. Pero cuando se gradúan y comienzan a realizar las tareas para las que se prepararon durante años, se dan cuenta que se enfrentan a dilemas morales que no se solucionan con una operación matemática o el diseño de un software. Algunos programadores se vieron ante situaciones que los condicionaba moralmente pero que al ser un trabajo lo realizaron, como es el ejemplo de aquellos que los presionan para crear páginas web que juegue con el precio de los productos dando un aumento gradual a fin de lograr que se compre cuanto antes, o un software para mejorar armas, entre otros.

El autor de la nota, Carlos Prego, comentó lo siguiente:

> Cuando en la coctelera se meten además cuestiones como la propiedad intelectual, la privacidad en el almacenamiento de datos o la legitimidad de acceso a un servidor, la necesidad de unas directrices éticas para los profesionales se vuelve si cabe más acuciante. (Xataka, 2019, "Ética y desarrollo software: el debate de si hace falta un juramento hipocrático para programadores", párrafo 6).

Luego Carlos Prego comenta una frase de Fernando Broncano[10] que es la siguiente:

> "Hay que desarrollar códigos de buenas prácticas y si es posible algún tipo de juramento hipocrático en general en todas aquellas ingenierías que sean

[9] Empresa de Ingeniería Electrónica
[10] Es un filósofo, fue profesor en la Universidad de Salamanca y actualmente profesor en la Universidad Carlos III de Madrid y autor de varios libros.

> sensibles" (Xataka, 2019, "Ética y desarrollo software: el debate de si hace falta un juramento hipocrático para programadores", párrafo 11).

En la nota también se plantea el interrogante "¿Un juramento como el de los médicos?" como respuesta a esto da cuenta que ya se ha intentado instruir a los desarrolladores en un juramento ético, pero observando actualmente entendemos que fracasó ya que no hay vigente un código ético.

En Estados Unidos se organiza el evento Data For Good Exchange cuyo objetivo principal es capacitar programadores para que cuenten con la capacidad de afrontar dilemas morales. [13]

7. Hacking

7.1 Definición

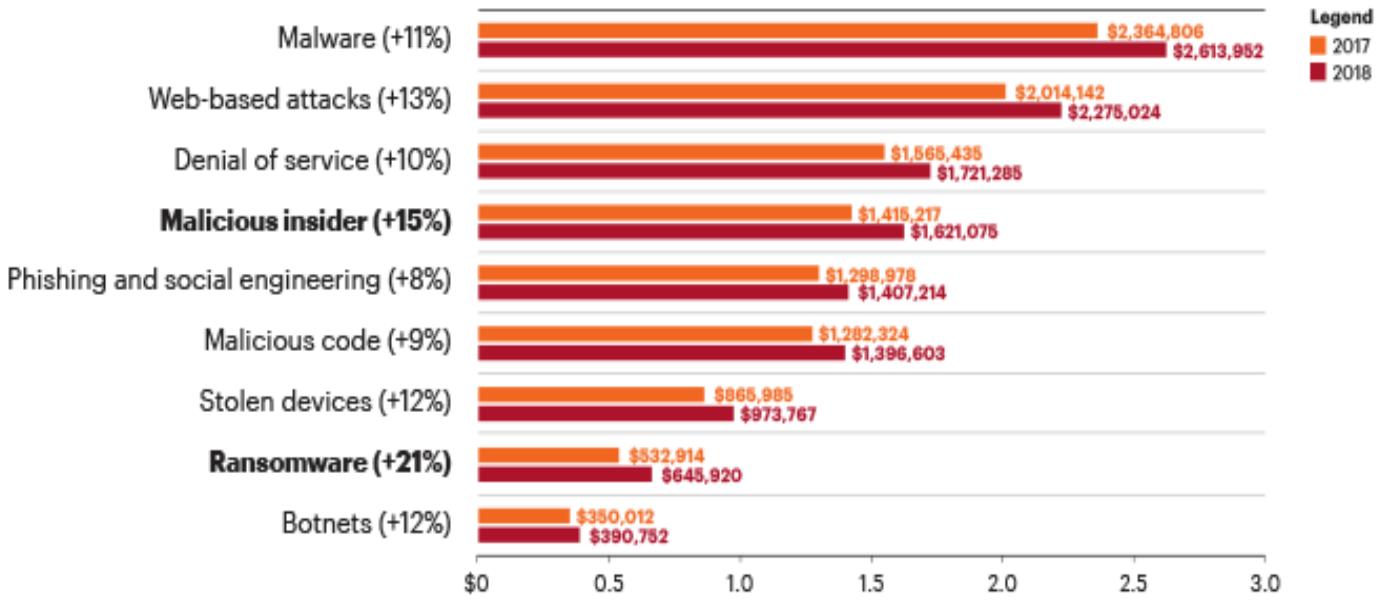
La mayoría de la gente cuando oye el término *hacking* lo entiende de una forma negativa, pero es preciso afirmar que esto no es así, sino que se debe a la cantidad de casos visibilizados de robo de identidad, datos, phishing y demás, es por ese motivo que la palabra hacking toma una connotación negativa. La definición correcta de hacking es la búsqueda de puntos vulnerables de redes, programas, sistemas y software a fin de localizar donde se encuentran y aquellos que emplean el *ethical hacking*[11] subsanan los puntos críticos, pero aquellos que no se dedican a la parte bondadosa del hacking aprovechan estas debilidades para robar datos, filtrar información entre otras acciones maliciosas.

7.2 Estadísticas de robos en línea

[11] El ethical hacking, también conocido como White hat (sombrero blanco) hace referencia al tipo de hacking autorizado que hace un experto del área de seguridad informática para detectar las vulnerabilidades que posee una empresa y repararlas.

A continuación, se observará una estadística desarrollada por Accenture en la cual muestra el avance de los delitos cometidos en línea que más se encuentran en aumento, en este caso el análisis entre el año 2017-2018.

Fig. 2 Gráfico estadístico sobre evolución de delitos más comunes en línea entre 2017 y 2018. [14]



7.3 Ransomware: hackeo a la Dirección Nacional de Migraciones de la República Argentina

Un grupo de ciberdelincuentes, hackearon los dispositivos electrónicos de la Dirección Nacional de Migraciones de la República Argentina logrando instalar un Ransomware[12], llamado Netwalker, a través del cual lograron extraer datos confidenciales que detallaban salidas y entradas al territorio Nacional y que tenía información relacionada con Interpol[13]. Se realizó con la intención de obtener un rédito económico ya que pidieron 4 millones de dólares para devolver los datos que fueron secuestrados. En total raptaron 22 carpetas que tenían 1,8 GB de datos que contenía también información referida a la Agencia Federal de Inteligencia (AFI).

Los hackers al no recibir la cifra solicitada ni una contrapuesta decidieron publicar los datos robados en la Deep web[14], sin tomar ningún tipo de reparo en las personas e instituciones que podrían verse perjudicadas, en especial aquellas destinadas a la seguridad Nacional Argentina (AFI) o a la seguridad internacional (Interpol).

7.4 Ataque cibernético contra el gobierno australiano

El primer ministro de Australia, Scott Morrison, denunció un ataque cibernético por parte de un agente estatal. El primer mandatario afirmó que el incidente afectó al gobierno, proveedores de servicios esenciales y empresas australianas. Scott Morrison dio cuenta que los ataques se encontraban en aumento en los últimos años y comentó que el año pasado los principales partidos de Australia y el Parlamento se encontraron envueltos en una "intrusión maliciosa" en sus redes computacionales. [15]

7.5 Naciones y organizaciones en la mira de los hackers

Los ciberdelincuentes han visto la oportunidad de vulnerar sistemas con mayor facilidad a raíz de la crisis sanitaria desencadenada por el Covid-19.

Entre los casos más destacados de hackeo se encuentra el de Italia, país en el que la página del Instituto Nacional de Seguridad Social (INPS) debió ser clausurada en el mes de marzo del corriente año, luego de que el acceso al sitio se viera comprometido tras una serie de ciberataques. Pasquale Tridico, titular de la dependencia gubernamental, informó que esta vulnerabilidad ocurrió luego de que hubo 339 mil aplicaciones para obtener un apoyo económico del Estado por parte de los ciudadanos.

En el Reino Unido una empresa especializada en estudios clínicos fue víctima de un ataque cibernético mediante el cual bloquearon miles de documentos de pacientes almacenados en la base de datos de la compañía.

El Departamento de Salud y Servicios Humanos de Estados Unidos (HHS) sufrió un ataque cibernético también en el mes de marzo del presente año. [16]

---

[12] es un software malicioso utilizado a fin de "secuestro de datos", que te bloquea el acceso a tus datos personales o empresariales.

[13] Organización Internacional de Policía Criminal refiere al mayor conjunto de policía Internacional con más de 190 países miembro.

[14] término mediante el cual se conoce a la internet "secundaria" u "oculta" a través de donde se conoce contenido que no aparecen en los motores de búsqueda convencionales, normalmente debido a que se publican elementos o productos ilegales.

Conclusiones

Luego de haber analizado las consecuencias de la utilización de datos, es evidente que: los datos personales y sensibles son en múltiples ocasiones vulnerados, los operadores tecnológicos se ven involucrados en aplicaciones de software malicioso y que las Big Tech no siempre realizan una utilización adecuada de la información de sus usuarios.

Como se puede observar en el punto tres en el cual se exponen cuatro empresas reconocidas en el ámbito tecnológico violan la privacidad de usuarios y clientes dejando expuestos datos personales y empresariales, lo cual se relaciona con el punto siete en el cual se detalla el concepto de hacking y como afecta a las empresas y Estados, en este caso en un contrapunto donde se ve que las entidades pueden ser víctimas también.

La investigación realizada y los ejemplos presentados dejan entrever que el uso indebido y la manipulación de datos ocasiona consecuencias graves.

En la economía de plataforma repasamos que los datos se utilizan como capital principal para llevar adelante este tipo de economía y que las empresas, big tech, la utilizan para valerse de datos personales y sensibles.

Se pudo determinar que nadie se encuentra exento de sufrir un robo o manipulación de datos. A su vez se resolvió que la tecnología se utiliza, en ciertos casos, con fines no éticos que impactan desde un punto de vista económico, político y social. Por otro lado, se estableció que el propio Estado sufre grandes ataques cibernéticos, pertenecientes en gran medida a empleados que traicionan la confidencialidad del gobierno.

Concluimos que es absolutamente necesario realizar un juramento hipocrático que contemple los siguientes principios:

1) Velar por el bien común y el bienestar de los clientes.

2) Proteger y respetar los datos que se le confíen.

3) Compartir los conocimientos que sirvan como avance el ámbito tecnológico

4) No utilizar las capacidades adquiridas para cometer delitos, violar derechos, ni, aunque sea intimado para realizarlo.

5) No diseñar programas que tengan por objetivo atentar contra terceros, empresas o Estados.

6) Desalentar la utilización de software para el avance de armamentos.

7) En absoluto realizar robo o secuestro de datos para obtener rédito económico.

"***No deberíamos dar por sentado que la evolución está guiada por algún tipo de providencia para alcanzar los mejores resultados éticos. Podríamos imaginar mejores resultados: humanos más inteligentes, altruistas y compasivos, por ejemplo. Tal vez sea eso lo que necesitamos hacer para proteger el futuro de la humanidad***" –

-Peter A. D. Singer- [15]

Referencias

[1] Mg. Lic. Darin Susana Beatriz (2020) *7 de julio Ética y RSE Problemática del Mundo Actual 2020 SDarin*. [Diapositiva 2]. Repositorio Material Facultad de Tecnología Informática.

[2]Vela, Fernández R. (23 de febrero de 2019). *La ética: una guía de la revolución tecnológica*. The Technolawgist. Recuperado el 9 de septiembre de 2020 de { HYPERLINK "https://www.thetechnolawgist.com/2019/02/23/la-etica-una-guia-de-la-revolucion-tecnologica/" }

[3] Protección de datos personales. (s.f.). *Datos personales: tus derechos.* Agencia de Acceso a la Información Pública. { HYPERLINK "https://www.argentina.gob.ar/aaip/datospersonales/derechos" }

[4]{ HYPERLINK "https://books.google.com.ar/books?id=Jti4fudh_cwC&pg=PA207&dq=que+es+la+tecnoetica&hl=es&sa=X&ved=2ahUKEwiU1qir0tPrAhW4IrkGHTobB5gQ6AEwA3oECAYQAg" \l "v=onepage&q=que%20es%20la%20tecnoetica&f=false" }

[5] Sorin, Sergio. (21 de marzo del 2000). *El habeas data en Argentina*. Equipo Nizkor. { HYPERLINK "http://www.derechos.org/sorin/doc/habeasdata.html" }

[6] Valdeolmillos, Celia. (7 de noviembre de 2019). *Un empleado de Trend Micro robó y vendió datos de 68.000 de sus clientes.* MC PRO. { HYPERLINK "https://www.muycomputerpro.com/2019/11/07/trend-micro-robo-vendio-datos-clientes" \l ":~:text=Noticias-,Un%20empleado%20de%20Trend%20Micro%20rob%C3%B3%20y,de%2068.000%20de%20sus%20clientes&text=La%20compa%C3%B1%C3%ADa%20de%20seguridad%20Trend,este%20pasado%20mes%20de%20octubre" }.

[7] Fang, Frank. (14 de junio de 2020). *Condenan a ingenieros por robar tecnología estadounidense de chips de Micron y transferirla a China.* La Gran Época. { HYPERLINK "https://es.theepochtimes.com/condenan-a-ingenieros-por-robar-tecnologia-estadounidense-de-chips-de-micron-y-transferirla-a-china_680391.html" }

[8] Página 12. (29 de enero de 2020). *Denuncian que Avast recopila datos de usuarios y los vende a grandes empresas.* { HYPERLINK "https://www.pagina12.com.ar/244557-denuncian-que-avast-recopila-datos-de-usuarios-y-los-vende-a" }

[9] Fernández, Javier G. (04 de septiembre de 2019). *Acusan a Google de dar en secreto datos personales de usuarios a los anunciantes.* Expansión. { HYPERLINK "https://www.expansion.com/economia-digital/2019/09/04/5d6fbef4e5fdea56148b4674.html" }

[10] Fundación Favaloro. (15 de junio de 2017). *Qué es el juramento hipocrático y que obligaciones determina.* { HYPERLINK "https://www.fundacionfavaloro.org/juramento-hipocratico-obligaciones-determina/" }

[15] Filósofo australiano profesor de derecho y filosofía en la Universidad de Monash.

[11] Cámara Argentina de Comercio y Servicios. *Las economías de plataforma* [Archivo de PDF]. { HYPERLINK "https://www.cac.com.ar/data/documentos/29_Econom%C3%ADas%20de%20Plataforma.pdf" }

[12] Moreno, Alfredo. (s.f.). *Datos y Algoritmos: el motor del Capitalismo de plataformas.* Motor Económico. { HYPERLINK "http://www.motoreconomico.com.ar/economia-mundial/datos-y-algoritmos-el-motor-del-capitalismo-de-plataformas" }

[13] Prego, Carlos. (22 de abril de 2019). *Ética y desarrollo software: el debate de si hace falta un juramento hipocrático para programadores.* Xataka. { HYPERLINK "https://www.xataka.com/legislacion-y-derechos/etica-desarrollo-software-debate-hace-falta-juramento-hipocratico-para-programadores" }

[14] Bissell, Kelly. Lasalle, Ryan M. Cin Paolo Dal. (6 de marzo de 2019). *Ninth Annual Cost of Cybercrime Study.* Accenture.{ HYPERLINK "https://www.accenture.com/us-en/insights/security/cost-cybercrime-study" }

[15] BBC News Mundo. (19 de junio de 2020). *Un "sofisticado hackeo de un agente estatal": Australia denuncia un ataque cibernético contra su gobierno.* BBC. { HYPERLINK "https://www.bbc.com/mundo/noticias-internacional-53102950" }

[16] Meza, Nayeli. Santillán, Ernesto. (8 de abril de 2020). *Naciones y organizaciones bajo ataques cibernéticos.* Reporte Índigo. { HYPERLINK "https://www.reporteindigo.com/reporte/naciones-y-organizaciones-bajo-ataques-ciberneticos-pandemia-covid-19-hospitales/" }

****Este trabajo ha recibido una mención especial en el Certamen de Trabajos Estudiantiles CIITI-TE 2020. Congreso Internacional en Innovación Tecnológica Informática.**