UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN

ABRIL 2022 - SEPTIEMBRE 2022

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN SISTEMAS DE INFORMACIÓN

TEMA:

La importancia del uso de las aplicaciones digitales para la protección de nuestros datos personales.

ESTUDIANTE:

Steeven Enrique Plaza Zapata

TUTOR:

Ing. Enrique Delgado Cuadro

AÑO 2022

CONTENIDO

PLANTEAMIENTO DEL PROBLEMA

En los tiempos contemporáneos, en nuestro diario vivir, es prácticamente imposible imaginarnos sin un dispositivo inteligente, sin una laptop, un smartphone, una smart tv, sin redes sociales, plataformas digitales. Podríamos decir que interactuamos en dos mundos, el mundo real y el mundo digital (o del internet, propiamente), siendo este último, uno que no terminamos de entender a profundidad y, sin embargo, si tratamos de imaginar un futuro sin él, sería como una distopía.

Dentro del mundo digital, también podríamos decir que indudablemente, de alguna manera, nos han facilitado la vida, podemos enviar mensajes instantáneos desde cualquier parte del mundo, transferir dinero, enterarnos de cosas que suceden en el mundo al instante, adquirir conocimientos de manera remota, es decir, cosas o actividades que antes nos tomaría un esfuerzo mayor, no obstante, ahora, ocupamos este mundo digital, internet, plataformas digitales la mayor parte del tiempo, dentro de este mundo digital, se han construido empresas enormes, que ofrecen servicios increíbles, muchas de ellas de manera "gratuita", pero, cada interacción, cada movimiento que nosotros hacemos dentro de este mundo digital genera datos, cada plataforma que ocupamos genera datos nuestros, cada foto que vemos, canciones que escuchamos, videos de observamos, nosotros estamos generando datos constantemente, pero, ¿Cuál es el fin de esos datos? ¿Quién es el propietario de los datos que nosotros generamos? ¿Tienen algún valor? ¿Cuál es la importancia de estos datos? ¿Deberían importarnos los datos que generamos en el mundo digital? ¿Deberíamos ser más cuidadosos con estos y protegerlos de alguna manera?

Ocupamos tanto el mundo digital que no nos detenemos siquiera a pensar en sus colaterales, es por eso el nacimiento de este caso de estudio. Nosotros, las personas no somos conscientes o somos poco conscientes de que nuestros datos son muy valiosos, es

un activo de mucho valor, es más, son una mina de oro gratuita para estas empresas contemporáneas, a pesar de ello, los usuarios que alimentamos bases de datos enormes que nutren de conocimientos a estas empresas, no tenemos ni idea el fin que tienen, el tratamiento que les dan y que tanto nos afectan a nosotros mismos.

JUSTIFICACIÓN

Ante el uso proliferante del mundo digital, los usuarios (nosotros) generamos datos todo el tiempo, cada movimiento, cada acción en el mundo digital genera un dato del cual se desconoce su fin, estos datos que generamos son muy importantes para las empresas, más aún, se apropian de ellos, resulta de especial interés conocer la importancia de los datos que generamos, de la importancia de su privacidad, y a partir de ahí, adoptar medidas para su protección, tanto de los datos propios que manipulamos en nuestros dispositivos inteligentes, como de los que generamos, tal vez, sin darnos cuenta.

El surgimiento de este caso de estudio pretende analizar la importancia que tienen nuestros datos, por lo general, usamos aplicaciones o plataformas en el mundo digital y no somos conscientes o creemos que no tienen ninguna importancia los datos personales que ingresamos a ellos o también pensamos que no es importante los datos que se generan al utilizar dichas aplicaciones, al realizar una búsqueda por internet, o el enviar un correo o un mensaje, pensamos que como somos civiles comunes, nadie está interesado en nuestros datos, no somos jefes de estado o empresarios de una multinacional, sin embargo, esos datos tienen mucho más valor que el que imaginamos, por lo que, también determinaremos el uso de alternativas de aplicaciones digitales para protegerlos los datos que generamos al usar internet.

Finalmente, este caso de estudio, busca proporcionar información relevante y de útil importancia para la comunidad en general, ya que todos compartimos el usar el mundo digital, con respecto a la importancia de tener una higiene de los datos nuestros y los que generamos.

Debido a que no es un tema popular el tener conocimiento de la importancia de nuestros datos, no se cuentan con una supremacía de estudios de alcance nacional al

respecto de la privacidad y protección de los mismos, este caso de estudio es conveniente para afianzar un mayor conocimiento e intervención sobre la manera que usamos el mundo digital.

OBJETIVOS

Objetivo general

- Analizar la importancia que tienen nuestros datos y el uso de aplicaciones digitales para protegerlos.

Objetivos específicos

- Describir la importancia de nuestros datos históricamente.
- Analizar el impacto que tienen nuestros datos en la actualidad.
- Determinar alternativas de aplicaciones digitales para la protección de nuestros datos.

LÍNEAS DE INVESTIGACIÓN

En cuanto al desarrollo de este trabajo investigativo, guarda relación con la línea de investigación sistemas de información y comunicación, emprendimiento e innovación, dentro de la sub-línea de redes y tecnologías inteligentes de software y hardware.

La concordancia de la línea y sublínea que se utilizó para el tema de este caso de estudio tiene que ver, ya que al tratarse de datos personales y la importancia de su cuidado en el mundo digital, implica a los sistemas de información y comunicación, además que, al ser un tema poco popular en estas épocas contemporáneas, alude a la innovación, y también, que, al protegerlos, nos adherimos a tecnologías inteligentes de software y hardware.

MARCO CONCEPTUAL

En la actualidad ocupamos internet todo el tiempo, y en torno a eso, se han desarrollado nuevas tecnologías, nuevos servicios y su proliferación es impresionante, se hacen más y más inteligentes, y nosotros las usamos todo el tiempo.

La mayoría de estos servicios, ofrecidos por internet, e incluso, el propio internet como tal se nos muestra de forma gratuita, lo cual nos lleva a pensar en ¿Cuál es su modelo de negocio? ¿Cómo se financian? Porque si de algo podemos estar seguros, es que no es barato tener servicios informáticos disponible y activos, más aún cuando estos están en todos lados, y los usamos todo el tiempo y es curiosos porque al usar todo el tiempo de manera gratuita un servicio o plataforma de internet, algún beneficio han de obtener estas plataformas.

"Si no pagas por el producto, entonces tú eres el producto" (Orlowski, 2020)

Si caminamos por la arena, junto al mar, vamos dejando las huellas de nuestros pies, nuestros pasos, que con el viento o las eas, se desvanecen, se pierden. Cuando navegamos por internet, también vamos dejando huellas, cualquier página que visitemos o algún tópico que tecleemos o investiguemos, todo eso va dejando huellas, esas huellas son datos, sin embargo, no sucede como los pasos en la arena junto al mar, en el internet, esas huellas no se desvanecen, se quedan perennes, esos datos son analizados, explotados y usados con un fin, desconocido para nosotros.

Esos datos que vamos dejando al ocupar internet ¿son nuestros? Nuestros datos, los que ingresamos para registrarnos y obtener una cuenta en cualquier página ¿son nuestros o la de página?

Para entender mejor este punto es menester comprender y definir:

¿Qué son los datos?

Aunque todas las definiciones apuntan al mismo lado, podemos tener distintas maneras de expresarlo.

Por una parte, tenemos que “Los datos representan un fragmento de una cantidad, medida, descripción o palabra, los cuales son agrupados o clasificados de una determinada manera para generar de información” (significados, 2022).

Cabe destacar que un dato por sí solo no representa valor, este debe ser analizado, procesado, con demás datos agrupados y ahí obtienen relevancia e información.

Otra definición que tenemos,

> Datos proviene del latín “Dtum” cuyo significado es “lo que se da”. Los datos son la representación simbólica, bien sea mediante números o letras de una recopilación de información la cual puede ser cualitativa o cuantitativa, que facilitan la deducción de una investigación o un hecho (Yirda, 2021).

Pensemos en algo, “Donald Trump”, eso es un dato, si no analizamos, obtenemos información, “Donald Trump fue ex presidente de los Estados Unidos” y este último se convierte en conocimiento, “Donald Trump fue el presidente N º 45 de los Estados Unidos de América”

El dato pasa a ser información y la información se convierte en conocimiento y esto es particularmente interesante e importante, ya que el conocimiento se transforma en poder.

El conocimiento y el poder siempre han guardado una relación muy cercana, y como ya mencionamos, que de los datos nace el conocimiento, quien tenga más datos

sobre nosotros, más poder tendrá sobre nosotros, con lo cual también podemos decir que el mientras más poder tengan sobre nosotros, es porque más conocimiento tienen sobre nosotros.

Las personas tenemos datos, además, siempre estamos generando nuevos datos, es más, nosotros somos datos, pero poco se nos concientiza sobre la importancia de los mismos, y no es casualidad que no estemos bien informados, que no sepamos valorar los mismos, ya que nuestros datos son el principal activo del mundo digital.

El nacimiento de los datos y un referente histórico

Nada se crea a partir de la nada, la explotación de los datos personales para la proliferación del poder a partir del conocimiento no es algo contemporáneo perse.

Históricamente, se conoce que los griegos fueron muy buenos para las matemáticas, y, por ende, las estadísticas, pero por sus creencias, no diseñaron un método de recopilación de datos.

En la era napoleónica, se comenzó a diseñar estrategias de guerra, política, económica, logística a partir de ciertas estadísticas que ellos diseñaban, recordemos que Napoleón fue un estadista y gran parte de su éxito se debe a que entendió que el conocimiento es poder.

Sin embargo, uno de los eventos históricos más importantes e impresionantes acerca del uso de la explotación de los datos lo encontramos durante la segunda guerra mundial.

Durante el régimen Nazi, mientras ocurría la segunda guerra mundial, el modus operandi de como los nazis invadían un país era apropiándose de los registros locales, ese era su primer paso para poder controlar a la población y, sobre todo, para localizar a su principal objetivo, los judíos, entonces, los nazis tuvieron una sed de datos personales locales, obviamente no todos los países tenían registros locales, esta diferencia marcada se puede notar entre Países Bajos y Francia de esa época. Un nombre importante y fundamental para que todo esto ocurriera fue Jacobus Lambertus Lentz o simplemente Jacobus Lentz, él fue un enamorado de las estadísticas demográficas, y fungía como inspector de registros de población holandés, cabe rescatar que él no era antisemita, sin embargo, hizo más por el régimen alemán que cualquier otro.

Lentz decía que "Registrar es vivir" y en marzo de 1940, dos meses antes de la invasión nazi, le propuso al gobierno de su país implementar un sistema de identificación personal que obligara a todos los ciudadanos a llevar un carnet de identidad, básicamente que todos tuvieran un sistema que lo siguiera desde la cuna hasta la tumba.

Para lograr el cometido, la tarjeta utilizaba tintas translúcidas que ocultaban a la luz de una lámpara de cuarzo, digamos, como un papel con marca de agua, esto con el fin de hacer difícil su falsificación. Al gobierno no le gustó la idea y lo rechazó, alegando que ese sistema va en contra de sus tradiciones democráticas, que sería tratar a las personas comunes como si fueran delincuentes. Obviamente Lentz se desilusionó, pero podríamos decir que no se dio por vencido. Unos meses después, lo volvió a intentar, pero esta vez a la Kriminalpolizei del Reich. Esta vez, esta propuesta de Lentz dejo fascinados a las fuerzas de ocupación y comenzaron a ponerla en práctica, entonces, todos los holandeses adultos pasaron a obligatoriamente llevar un carnet de identidad, y, en caso de ser judío, llevaban una J, osease, básicamente, una sentencia de muerte en sus bolsillos.

Lentz, además de los carnets, también utilizó máquinas Hollerith, para ampliar la información registrada sobre la población.

Entonces, siguiendo con la historia, en 1941 se emitió un decreto que, en suma, obligaba a todos los judíos a registrarse en su oficina local del censo. Durante el pasar de las décadas, los holandeses habían recopilado, talvez de forma inocente, datos personales de los ciudadanos, como la religión, sexo entre otras cosas, para poder darle seguimiento a cada persona, desde que naciera hasta que falleciera, esto con la ayuda de las maquinas Hollerith y claro, con todo esto, a los nazis se les hizo muy sencillo ubicar personas.

Por otra parte, diferente a lo que se estaba haciendo en Países Bajos, en Francia, el método de censar no a sus ciudadanos, no admitía o no requería la información de datos sobre religión, por razones de privacidad. La última recolección de datos a base de censo se había dado en 1872. Henri Bunle, que era el jefe de la oficina de Estadística General francesa, manifestó muy firme a la Comisión General sobre Asuntos Judíos en 1941 que Francia desconocía cuántos judíos tenía y, más aún, dónde vivían. Además, es importante recalcar que Francia no contaba con la amplia infraestructura de tarjetas perforadas que, si tenía Países Bajos, lo que suponía una mayor dificultad a la hora de la receptación de nuevos datos, entonces, si el régimen nazi quería que la policía censara a la población, esa recopilación de datos se tendría que llevar manualmente, con papel y cartulina.

No se podía computar ni encasillar los datos que se recolectaban de los ciudadanos ya que no se contaba con las tabuladoras Hollerith, lo que llevó a la desesperación a los nazis. René Carmille, fungía como auditor general de del ejército francés, además era un encantado de las tarjetas perforadas y en su poder contaba varia maquinas tabuladoras (y una que otra Hollerith), él se ofreció voluntariamente para alivianar el problema y entregar aquellos valiosos datos (judíos) a los mencionados nazis.

René desarrolló un número nacional de identificación personal, su función era como un código de barras descriptivo de cada ciudadano, podemos argumentar que fue el precursor del actual número de seguridad social francés. Dependiendo de las características personales, como la profesión, se asignaban diferentes números, además Carmille también fue el responsable del censo de 1941 para todos los ciudadanos franceses con un rango de edad entre los 14 y 65 años de edad. Dentro del cuestionario del censo, existía una pregunta, la pregunta número once, que pedía a los judíos que se identificaran por medio de sus abuelos maternos y paternos y también de la religión que seguían.

Mientras transcurría el tiempo, los nazis estaban a la espera de la lista de judíos de René del proporcionaría, pero que no llegaba, esto provoco que los nazis se impacientaran y empezaran con las redadas contra los judíos en parís, mas, sin embargo, sin los datos tabulados y clasificados de Carmille, los nazis dependían de que los judíos se entregasen por sí mismos o que alguien más los delatara, pasaron los meses y las listas de Carmille seguían sin llegar.

René Carmille no tenía intención alguna de traicionar a sus ciudadanos, pero los nazis no sabían eso. Fue uno de los más altos cargos de la Resistencia francesa. Esa operación generó alrededor de unas 20000 identidades falsas, pues usó las tabuladoras de su poder para identificar a los individuos que estarían dispuestos hacerles frente a los nazis. Aquella respuesta número once jamás fue tabulada, esos datos se perdieron para siempre ya que nunca se perforó esos agujeros. En estos tiempos contemporáneos, se han descubierto más de cien mil de las tarjetas perforadas falsificadas de esa época. Y si, esas tarjetas jamás fueron entregadas a los nazis, y ese sutil acto de una sola persona, de no recopilar esos datos, datos tóxicos, salvó a cientos de miles de personas.

Obviamente Carmille sabía que el no cumplir con el cometido, traería consecuencias, que tarde o temprano los nazis se darían cuenta y así fue, lo arrestaron en 1944, lo torturaron dos días y luego lo mandaron a Dachau y después de un año, falleció de extenuación. La tasa de mortalidad de los judíos en Holanda fue del 73%, mientras que en Francia fue del 25%. La recopilación de datos puede matar y el mejor indicador de que algo ocurrirá en el futuro es que haya ocurrido en el pasado (Véliz, 2021).

Propiedad de los datos

Es lógico pensar que los datos que genera el individuo de sí, son información privada, que le pertenecen al individuo perse, sin embargo, al usar una aplicación, por ejemplo, de delivery, los datos que generamos como preferencias personales hacia un producto, ubicación entre otros, son explotados por la aplicación de delivery para generar ingresos, pero esos datos están completamente relacionados con el individuo, entonces, bajo ese concepto, esos datos que el usuario generó ¿son del usuario o de la empresa de delivery?

Las empresas titanes del mundo digital, como Google, Facebook, Microsoft, Amazon, nos quitan "voluntariamente" nuestros datos a cambio de entretenimiento y atención, nuestros datos valen mucho, prácticamente su economía se basa en nuestros datos de los cuales no recibimos nada, además que, aparte de los datos que voluntariamente entregamos, también pasan recolectando datos, sin necesariamente nos demos cuenta y aplican minería de datos, "El minado de datos es un conjunto de técnicas y tecnologías que permiten explorar grandes bases de datos, de manera automática o semiautomática, con el objetivo de encontrar patrones repetitivos que expliquen el comportamiento de estos datos" (Bello, 2021).

Definir la propiedad dentro del mundo digital es un nuevo dilema, del cual se aprovechan con audacia, *¿Cómo nació la propiedad?* Cuando se construía nuestra sociedad, y comenzaron a emerger las clases sociales, básicamente, se convertía en propiedad lo que se podía tocar, un individuo tocaba una silla y podía decir, esta silla es mía, así nació la propiedad, sin embargo, ¿Podemos tocar un dato? ¿Podemos tocar un flujo de información? Entonces, en el mundo digital pasamos del concepto de propiedad al concepto de usufructo.

"El usufructo es el derecho real de goce o disfrute de un bien que no nos pertenece, o sea, de una cosa ajena. Esto se traduce en términos jurídicos a la tenencia de la cosa, más no a su propiedad" (Etecé, concepto.de, 2020)

Esto nos convierte en usuarios, y poco a poco somos más usuarios que ciudadanos como tal, hasta cierto punto, no está mal que empresas privadas almacenen nuestros datos, pero, que exploten y monopolicen esos datos, eso sí es peligroso, y es algo que poco se regula, ya que el estado tendría que pasar de la regulación de la propiedad a la regulación de la aplicación de esos datos. Es por eso que Facebook puede suspender "tu" cuenta, donde ingresas "tus datos", entonces si alguien más tiene poder de algo que te pertenece, no es tuyo.

No es normal que estas empresas tengan tantos datos personales nuestros, sin regulación, como ya lo mencionamos, mientras más datos tengan de nosotros, más conocimiento tienen, y el conocimiento es poder y entonces, ellos tienen demasiado poder, por eso es menester la privacidad de los mismos.

¿Qué es la privacidad de los datos?

Ya sabemos que son los datos, ya entendemos que hay que preocuparnos por su privacidad, así que partamos definiendo qué es privacidad en sí:

> La privacidad es todo lo relacionado con la vida personal de cada persona y que debe mantenerse de forma íntima y secreta. Un individuo tiene derecho a tener privacidad en su vida, es decir que la persona puede realizar acciones, que no necesariamente, tenga que compartir con los demás (Redacción, 2021).

De alguna manera, somos transparentes, vulnerables para las empresas, pero las empresas no son transparentes hacia nosotros.

"La privacidad de los datos es la protección de los datos personales frente a quienes no deberían tener acceso a los mismos, y la capacidad de los usuarios de determinar quién puede acceder a su información personal" (cloudflare, s.f).

Pensemos en una empresa como Google, alguien como Google no solo tiene mucho acceso conocimiento (porque tiene mucho poder), sino que también elije que cuenta como conocimiento de ti y con eso te encasilla en una caja de categorizaciones, es decir, género, edad, salud, poder adquisitivo, religión, creencias, gustos, y es un hecho que nos conoce mejor de como nosotros nos conocemos perse y en esta era digital esto se ha proliferado increíblemente porque nunca habíamos tenido tanta habilidad para recopilar datos y analizarlos, como los tenemos ahora.

"Cualquiera que tenga acceso a su información puede apropiarse de su identidad. Por lo tanto, mantener la privacidad de los datos privados y las categorías especiales de datos es fundamental para proteger la identidad" (McAfee, 2020).

Si no tenemos seguridad, no tenemos privacidad y viceversa.

¿En qué se basa el modelo de negocio del internet?

El internet como tal es gratuito, no se cobra por usarlo, tal vez paguemos la banda ancha, o un plan para navegar, pero el acceder como tal es gratuito, ¿Cómo se financia? Pues, la mayor parte del internet está financiado por un modelo de negocio que depende de la violación sistemática y masiva de derechos, sobre todo, los de privacidad, lo cual no es normal ni tampoco debería de ser aceptable, pues los inmensos servidores de las grandes empresas que entre si permiten el funcionamiento del internet, no se mantienen de la nada.

¿Cuál es el modelo de negocio de las empresas más importantes?

Este tópico está fundamentalmente relacionado con el anterior, y es que, en suma, el modelo de negocio de las empresas más importantes como Google, Facebook, Amazon, es muy frágil, ya que depende en gran medida de nuestros datos personales, esos que generamos en todo momento y por el cual nos dan (u obligan a consumir) entretenimiento y atención.

Hacen todo lo posible para obtener aún más datos personales (como esos juegos de “descubre al amor de tu vida”, o “descubre lo que revela tu signo”). Es por eso que, aunque son multinacionales, hacen tanto marketing, porque se sabe frágil, así las demás.

Pensemos un momento en Facebook, en realidad Facebook no es una página o aplicación en la que uno comparte memes y cosas así, Facebook sirve para desestabilizar democracias, es donde está la mayor ganancia, ahí es donde gastan esfuerzos y personal, es impresionante la capacidad, el poder, la injerencia que puede tener Facebook sobre cualquier elección presidencial, sobre todo las de Latinoamérica, los datos personales que se recopilan de Latinoamérica, son los que más valen, porque son las democracias más

baratas en desestabilizar, además que cuentan con recursos naturales, capital humano que son muy aprovechable para el primer mundo, sobre todo el americano.

Atravesamos por una pandemia de información y de infodemia, desinformación y libertad de expresión.

El modelo de negocio que depende de la explotación de datos personales es demasiado tóxico para la sociedad.

Incluso, el reconocido historiador Yuval Noah Harari (2018) afirma:

> La carrera para poseer los datos ya ha empezado, encabezada por gigantes de los datos como Google, Facebook, Baidu y Tencent. Hasta ahora, muchos de estos gigantes parecen haber adoptado el modelo de negocio de los «mercaderes de la atención». Captan nuestra atención al proporcionarnos de forma gratuita información, servicios y diversión, y después revenden nuestra atención a los anunciantes. Pero las miras de los gigantes de los datos apuntan probablemente mucho más allá que cualquier mercader de la atención que haya existido. Su verdadero negocio no es en absoluto vender anuncios. Más bien, al captar nuestra atención consiguen acumular cantidades inmensas de datos sobre nosotros, que valen más que cualquier ingreso publicitario. No somos sus clientes: somos su producto (pág. 100).

Cualquiera puede crear una empresa y diseñar un algoritmo destinado a lo que sea, publicarlo, mostrarlo al mundo, sin el temor que alguien le supervise, es increíble, no podríamos sacar al público un suplemento o medicina, pero si una aplicación que recopile y explote datos de millones de personas, analice y decida si alguien puede acceder o no a un lugar, si es acreedor de un préstamo o no, si debe ir a la cárcel o no.

Vigilancia, control y actualidad.

En este punto, cada vez más nos queda claro que los datos son muy importantes, es más, en la actualidad, es el recurso de mayor valor.

Angela Merkel (2018) manifestó en el Foro Mundial Económico "Los datos son la materia prima del siglo XXI" esto ante su preocupación a la Unión Europea a actuar sobre la protección de los datos.

La prestigiosa revista The Economist, en su edición "Fuel of the future" (2017) afirma:

> Los datos son a este siglo lo que el petróleo fue al anterior: un motor de crecimiento y cambio. Los flujos de datos han creado nuevas infraestructuras, nuevos negocios, nuevos monopolios, nuevas políticas y, lo que es más importante, nuevas economías. La información digital es diferente a cualquier recurso anterior; se extrae, valora, compra y vende de diferentes maneras. Cambia las reglas de los mercados y exige nuevos enfoques de los reguladores. Se librarán muchas batallas sobre quién debe poseer y beneficiarse de los datos (pág. 19).

El único problema de comparar un recurso tangible con uno intangible, es que, como lo mencionó Franklin Foer (2017) "Los datos no se parecen al petróleo. El petróleo es un recurso finito; los datos son infinitamente renovables. Permiten continuamente que el nuevo monopolista lleve a cabo experimentos para dominar la previsión de las tendencias, para entender mejor a los consumidores, para construir algoritmos superiores" (pág. 183).

Con la era digital se está creando un nuevo poder, que es el de la capacidad de adelantarse al comportamiento humano, tener tantos datos acumulados, guardados,

analizarlos y explotarlos, saber tanto sobre las personas que pueden influir en su comportamiento, ¿Todas las decisiones que tomamos, de verdad son nuestras?

Mientras estamos conectados a Facebook, todo se rastrea, cada click, cada publicación que no publicamos, cada perfil que visitamos, y no solo eso, como la mencionada red social tienen acceso a nuestro teléfono, ubicación entre otros cien número de cosas, hasta las llamadas y SMS, junto con un gran algoritmo, en la sección de 'personas que quizás conozcas', como por arte de 'magia' nos aparece hasta el desconocido que saludamos hace unas horas, la propia red social junta personas, que en algunas ocasiones, resultan ser conexiones problemáticas, fabrica conexiones de víctimas, victimarios, amantes, delincuentes, es un tema escabroso en realidad.

Uno de los escándalos más escandalosos fue el de Facebook con Cambridge Analytica, un punto de inflexión que nos demuestra que los datos sí son la materia prima de la humanidad actual.

Cambridge fue una empresa creada en el 2013, su fuerte era la minería y análisis de datos, esta había colaborado en varias campañas políticas, ya que "habría empleado su plataforma para obtener de forma ilegal los datos de 87 millones de usuarios que utilizaban Facebook. Estos fueron utilizados en las elecciones presidenciales de Estados Unidos para que Donald Trump llegara a ser presidente" (Frutos, 2018).

Cambridge recopiló los datos privados de los usuarios de Facebook (cosa que la red permitía libremente en ese entonces) y solo hacía falta que un usuario concediera permiso para que, sin el consentimiento de tus demás amigos, ellos también pudieran recopilar esos datos.

"Cambridge Analytica, a través de una aplicación aparentemente inofensiva que hacía un supuesto test de personalidad (Thisisyourdigitallife), pagó en 2013 para que

270.000 usuarios hicieran el test, dando acceso además a los datos de todos sus amigos" (Gonzáles, 2018).

Con eso, la empresa analizadora, con toda su recopilación que, el test lo hicieron 270.000 usuarios, pero con esto de que también tenían acceso a los datos de tus amigos, suma unos 87 millones en total, mediante la explotación de esos datos, pudieron generar, digamos, un arquetipo de modelos de votantes potenciales y así personalizar el contenido y publicidad para que funcione, dependiendo del usuario como tal, y así, llevar a personas al poder.

Por otra parte, Facebook también dio vía libre a que muchas firmas tecnológicas (150 aproximadamente), incluida las titánicas, tuvieran acceso a los datos personales, privados, incluso a los mensajes privados y que hasta los pudieran borrar, todo esto sin el consentimiento, sin el permiso (claro está) de sus usuarios.

"La red social compartió más datos personales de sus usuarios con empresas tecnológicas como Microsoft, Amazon, Spotify o Netflix de los que se habían dado a conocer hasta ahora, lo que permitió consultar incluso los mensajes privados de los usuarios" (Sánchez, 2019).

Además:

> Otras aplicaciones como Bing, el buscador de Microsoft, ha sido capaz de encontrar los nombres de todos los amigos y contactos de los usuarios de Facebook sin su consentimiento. Según el diario americano (The New York Times), otras empresas como Amazon y Yahoo también han tenido acceso a nombres de usuarios, publicaciones, información de amigos y publicaciones de nuestros contactos (Muñoz, 2018).

Hablemos también sobre una de las aplicaciones más usadas, propiedad de Facebook (que ahora es Meta), WhatsApp.

WhatsApp es enorme, de hecho, "WhatsApp tiene más usuarios que habitantes hay en China, 2.000 millones de personas" (Alpañés, 2021).

El problema radica en que la aplicación como tal es más íntima, redes sociales es como un parque, WhatsApp una habitación, no hay brecha para ponerle anuncios, lo cual representa muchos problemas para el capital, es por eso que la plataforma sea como fuere, cada vez más está dejando de ser íntima perse, deliberadamente Zuckerberg, creador de Facebook, ha buscado maneras de poder relacionar los datos de WhatsApp con Facebook, no con tanto éxito por la Unión Europea y su Reglamento General de Protección de Datos (RGPD), pero, esto solo frena las cosas en Europa. En nuestro continente buscan con fervor poder relacionar los datos de WhatsApp con Facebook.

Es extremadamente peligroso que los datos de una plataforma con la que interactuamos de forma íntima, sean estudiados, analizados y posteriormente explotados sin nosotros darnos cuenta.

La plataforma cuenta con un cifrado de extremo a extremo, sí, pero tiene otras formas de obtener información:

> Pero hay información valiosa más allá del contenido del mensaje, en los metadatos: quién habla con quién, cuándo, dónde, desde qué teléfono, matiza Harry Halpin, profesor del Instituto de Tecnología de Massachusetts, director de Nym, una empresa de protección de datos, y autor de Social Semantics: The Search for Meaning on the Web (Semántica social: la búsqueda de significado en la web). Estos metadatos ayudan a crear un perfil bastante preciso del usuario, subraya Halpin,

> crítico con Zuckerberg: "Casi 3.000 millones de personas usan Facebook y 2.000 millones usan WhatsApp [otros 1.000 millones, Instagram]. Al menos una cuarta parte de la vida humana consciente está bajo vigilancia por su parte. Es inaudito históricamente. Y da poderes inimaginables para intentar monitorear, manipular y controlar" (Alpañés, 2021).

No es normal ni aceptable estar sumergidos en una vigilancia tecnológica, y, sobre todo, que una sola persona, o ente tenga demasiado conocimiento, demasiado poder ¿Cuánto nos cuesta el mandar memes a nuestros amigos?

Ahora bien, aunque Facebook y su ecosistema sea potencialmente la más peligrosa y peor red social, no es la única que tiene las manos sucias.

Al navegar por internet, como ya se mencionó al inicio de este trabajo de investigación, vamos dejando huellas, todo lo que hacemos va dejando rastros por ahí, a esto también se lo conoce como Huella del dispositivo.

"Podemos decir que la huella digital es el término que engloba a los registros y rastros que dejamos cuando cogemos un dispositivo y navegamos por Internet. Es información de los usuarios que puede ser utilizada por terceros" (Jiménez, 2022).

Todos estos registros, que incluyen datos personales y que dejamos expuestos, estos datos, registros, correlacionados, analizados y después encasillados.

Esto se relaciona también con que, cada vez que vamos navegando, se van creando cookies. Una cookie es un fragmento de información que la página web envía al dispositivo y contiene información de navegación.

Las cookies pueden "Recordar accesos y conocer hábitos de navegación. Las cookies hacen que las páginas web puedan identificar tu ordenador, y, por lo tanto, si

vuelves a entrar a ellas podrán recordar quién eres y qué has hecho antes dentro de ellas" (Fernández, 2020).

Estas cookies que van creando distintas páginas, también pueden ser solicitadas por las páginas, entonces, mediante un rastreo de cookies se va generando una especie de Gran ID, donde nos tienen básicamente vigilados, es decir, saben todo sobre nosotros, mejor que nadie, es increíble.

Y si le sumamos a eso que todos también tenemos un Id de Publicidad, en nuestros distintos dispositivos y que, mediante las cuentas de registro, todo se conecta.

En este ID, ya no nos debe sorprender, se monitorea todo, en qué apps pasamos más tiempo, temas de interés, búsquedas, a qué hora comenzamos actividad en nuestro dispositivo y cuando dejamos de utilizarlo, mucha información que esta en vigilancia y se es compartida con todas las apps que descargamos.

Todo es smart, smart tv, smartwatch, smartphone, smarttag, asistente inteligente en casa, en fin, todo recopila datos, todo lo que hacemos, lo que decimos, porque ellos también acceden a nuestros micrófonos, a nuestras conversaciones privadas, estamos vigilados constantemente, con el fin de ser más efectivos al vendernos algo, en hacernos comprar algo, en adelantarse al comportamiento humano, en manipularlo, en convertirnos simplemente en consumidores, y claro, otros fines desconocidos para nosotros, también existen los carros smart, los carros inteligentes, saben tus recorridos, tu rutina, lo saben todo.

Google, por medio de todos sus servicios, conoce todo lo que haces, con Gmail conoce tu fecha de nacimiento, nombre, edad, sexo, e incluso tus ideologías, con Google Documents sabe tus faltas ortográficas, tu retórica, Google Maps, tu ubicación, lugares que frecuentas, donde vives, donde trabajas, donde estudias, y que tiempo le das a cada

lugar, entre otros, Google Keep, todo lo que piensas, y con eso, muchas deducciones, Google también sabe todo lo que consultas, lo que te gusta y lo que no, lo que quieres comprar y lo que no, las fotos que te gustan, lo que lees, e incluso eso que consultas en modo incognito, con el Drive, conoce toda tu información, con el Google Calendar, sabe tu rutina, eventos, fiesta, es decir, lo que tienes planeado, además, con otros servicios (asistente, Android, entre otros) conoce tu rostro, tus ojos, conoce tu huella dactilar, también conoce el timbre de tu voz, como hablas, lo que dices.

Amazon, la tienda más grande del mundo, te vende de todo, conoce tus gustos, lo que lees, tu dirección, conoce tus conversaciones mediante Alexa, esto es escalofriante, por cualquier lado que se lo vea, además, con su plataforma y su Marketplace, otros proveedores se registran y venden en Amazon, entonces con esas métricas, Amazon analizaba cuáles eran los productos más vendidos, los replicaban ellos o compraban esos productos al fabricante, lo vendían a precios ridículos, y esa centralización origina destruir a la competencia, cambian la economía y obtienen todo el poder, y aparte de eso, también Amazon concentra las pág. digitales, Amazon o AWS es el proveedor más grande de almacenamiento de servicios, páginas web, base de datos y un cien número de cosas más.

Como podemos darnos cuenta, estas empresas que recopilan datos sin nuestro permiso, no han sido nada transparentes y no nos comentan a ciencia cierta, cual es el fin de su gran interés con respecto a nuestros datos.

> Tener una vida privada en el mundo digital “cada vez es más difícil, por no decir imposible”: “Desde que nos conectamos, nuestros operadores mantienen los datos de conexión, utilizamos sistemas gratuitos y aceptamos esos rastreos. Existen las cookies, los asistentes de voz, cámaras de videovigilancia…”. Y en muchas ocasiones es el propio usuario el que

> aporta “una mayor riqueza de datos al publicar todo lo que hace en redes sociales y participar en retos como el #10yearschallenge o descargar aplicaciones como FaceApp” (Rubio, 2019).

Si nuestros datos se los damos a empresas privadas, mandarán los ricos, si se los damos al gobierno, sufriremos de autoritarismo y fascismo.

> Si queremos evitar la concentración de toda la riqueza y el poder en manos de una pequeña élite, la clave es regular la propiedad de los datos. En tiempos antiguos, la tierra era el bien más importante del mundo, la política era una lucha para controlar la tierra y evitar que se concentrara demasiada en unas pocas manos, la sociedad se dividía en aristócratas y plebeyos (Harari, 21 lecciones para el siglo XXI, 2018, pág. 99).

Aparte de lo que podemos hacer individualmente, nos hace falta cuanto antes una regulación importante, a nivel gubernamental, porque como ya lo mencionamos anteriormente, no es posible que no exista ningún tipo de regulación, podemos crear un algoritmo y nadie nos supervisará. Es bastante peligroso el que estemos vigilados constantemente, que recopilen nuestros datos personales, todo lo que hacemos, interactuamos, leemos, en fin, tienen mucho conocimiento sobre nosotros, nos conocen mejor que nosotros mismos, y eso conlleva a que también tengan mucho poder sobre nosotros, eso nos hace muy vulnerables.

Alternativas para la protección de nuestros datos.

Debemos de proteger nuestros datos, el primer paso es tener responsabilidad en los datos que compartimos, además de lo que permitimos que sea compartido ya que cualquier cosa que compartamos será pública, y el hecho que sea pública significa que nos estamos exponiendo y una vez que compartimos algo en internet, no hay vuelta atrás.

Además, dentro del mundo digital también podemos utilizar aplicaciones digitales para la protección de nuestros datos, existen aplicaciones, alternativas con las cuales protegernos, no solamente los titanes ya establecidos. A continuación, se mostrará una tabla con las mejores herramientas digitales para la protección de nuestros datos.

Tabla 1: Compendio de herramientas seguras para la protección de nuestros datos personales.

Alternativas seguras para consultas en la web.		
DuckDuckGo	Al igual que Google Search es un motor de búsqueda, se centra en la privacidad, no rastrea las búsquedas ni recopila datos, garantizan la máxima privacidad	No recopila datos, ni la dirección IP, además, tampoco comparte los datos recopilados con las páginas accesadas, no personaliza resultados, tampoco guarda el historial de búsquedas y tiene un cifrado más seguro.
Starpage	"Fundada en 1998 como Ixquick.com, con el tiempo se convirtió en Startpage.com y en 2006, crearon "el motor de búsqueda más privado del mundo", el cual no registra, rastrea ni comparte tus datos personales" (José, 2021).	No comparte datos, no recopila metadatos ni datos personales ni información de identificación. Permite el consultar páginas webs de manera totalmente anónima, ya que ellos cuentan con su propio proxi.
Alternativas seguras para el ámbito de los correos electrónicos.		
ProtonMail	"Es un servicio de la empresa Proton Technologies AG que tiene su sede en Suiza. Esa compañía fue creada en 2013 por Jason Stockman, Andy Yen y Wei Sun, ingenieros y científicos que trabajaban en el CERN" (Solé, 2021).	Es una alternativa gratuita que ofrece como una gran ventaja su seguridad y privacidad, se orienta a la privacidad y el cifrado de extremo a extremo de acceso cero (ni ellos tienen acceso al contenido), no permite la vigilancia.
Tutanota	Es un proveedor de correo electrónico que se enfoca en la privacidad, cuenta con cifrado de extremo a extremo que hace que su interceptación sea casi imposible, es de código abierto y muy simple de usar.	Protegen la identidad del usuario al no almacenar registros ni requerir información personal al momento de registrarse, cuenta con su sede en Alemania, lo cual aporta una ventaja adicional, por las jurisdicciones del país.
Alternativas seguras a nivel de navegadores.		
Brave	Es un navegador gratuito que prioriza la privacidad de sus usuarios, es de código abierto y está basado en el Chromium, cuenta con un bloqueador de anuncios y obliga a las páginas web usar conexiones seguras.	"No almacena datos personales ni información de navegación en los servidores, sino que esto se queda almacenado en tus dispositivos hasta que tú decides eliminarla. No se vende la información a terceros" (García, 2021).
	"Es un navegador de Internet que permite a los usuarios navegar por la web anónimamente. También te da	Cuenta con un cifrado muy efectivo, es de código abierto y su principal objetivo es proteger la privacidad y seguridad de los

Tor	acceso a la dark web. Tor es una red mundial de servidores diseñados específicamente para la comunicación privada" (Sherman, 2020)	usuarios, tanto así que algunas páginas no funcionan bien, porque no pueden capturar nuestros datos y eso lo convierte en un navegador un poco lento, pero seguro.
LibreWolf	Es un navegador de código abierto, una bifurcación independiente de Firefox, también es uno de los navegadores más seguros, bloquea cookies de seguimiento y ayuda a disminuir la recopilación de huellas de navegador.	Una de sus principales llamativas, es que no recoge datos de telemetría, ni tampoco recopila datos para después venderlos al mejor postor, también bloquea la publicidad e incorpora un cortafuegos, tampoco utiliza conexiones en segundo plano por defecto.
Para brindarle seguridad a la conexión a internet como tal podemos usar VPN. VPN o red privada virtual, en términos simples, tener una vpn nos ayuda a cifrar la conexión del dispositivo al que se accede al destino, es decir, aporta seguridad a esa conexión, que no puedan interceptar esos flujos de datos.		
ProtonVPN	Pertenece a la familia de ProtonMail (del cual se habló anteriormente) es un vpn muy seguro, prácticamente lo que ya se comentó acerca de ProtonMail, comparten su idiosincrasia por la seguridad.	
Mullvad VPN	Un vpn muy seguro y de bajo costo, es extremadamente segura, tanto por sus amplias configuraciones como por su jurisdicción, ya que su sede está en Suecia.	Probablemente una de sus desventajas sea que no desbloquea contenido restringido por países en los servicios de streaming, en otras palabras, no desbloquea el catálogo de Netflix de los Estados Unidos.
ExpressVPN	"permite la protección de datos contra los hackers y ladrones de identidad. Con esta VPN se puede esconder la dirección de IP del usuario, sin que terceras personas puedan observar lo que se hace dentro de la red" (trucoslondres, 2020).	Destaca porque puede acceder a contenido, entretenimiento sin ningún tipo de restricciones, además que permite ser anónimos en cuestión de segundos, aunque cabe mencionar que esta vpn es una de las más costosas del mercado.
Alternativa segura en el área de almacenamiento en la nube.		
Netxcloud	Es un servicio de alojamiento de código abierto, con ella podemos tener todos nuestros archivos disponibles en cualquier momento y lugar, además que ofrece una alta seguridad.	Cuenta con un amplio ambiente de funcionalidades, editor de texto, calendario, gestor de notas, gestor de contraseñas, reproductor de música, mapas, entre otros.
Debemos de proteger nuestras contraseñas, una alternativa segura.		
Bitwarden	Ofrece el gestionamiento de contraseñas, su principal fuerte es la privacidad y seguridad. Está disponible para los principales S.O y también se puede agregar a los principales navegadores, lo cual nos permite que Bitwarden, desde el navegador, gestione y genere contraseñas.	Las contraseñas creadas con Bitwarden "son muy difíciles de descifrar, aunque se utilice la fuerza bruta. «Bitwarden realiza auditorías de seguridad de terceros con regularidad y cumple con los estándares de seguridad Privacy hield, HIPAA, GDPR, CCPA, SOC2 y SOC3»" (González, 2022).

Doble Factor de Autenticación (2FA), dotaremos de mayor seguridad el acceso a nuestras cuentas.		
Authy	Es un servicio 2FA, doble autenticación, gratuito, y que nos ayuda a aportar mayor seguridad al ingreso de nuestras cuentas, además que su manejo y autenticación es fácil de utilizar.	
Microsoft Authenticator	Desarrollada por Microsoft, nos ayuda con el mismo cometido, verificar mediante otro dispositivo si somos los propietarios de la cuenta.	
Yubico	Esta alternativa es un poco diferente a las dos anteriores mencionadas, es decir, el proceso en el mismo, es 2FA, sin embargo, esta consiste en un dispositivo físico, como una memoria USB, donde la verificación se completa al introducir el mencionado dispositivo.	
Alternativas seguras de mensajería.		
Signal	Es una aplicación de mensajería como WhatsApp, pero se centra en la privacidad, es gratuita y de código abierto, también incluye esas herramientas que usamos todo el tiempo como llamadas, grupos, emojis, videollamadas.	Cuenta con un cifrado de extremo a extremo (que WhatsApp luego incorporo), pero el cifrado de Signal es más seguro, se llama Open Whispers Systems, básicamente el mensaje se cifra y se envía, el dispositivo que recibe lo descifra.
Session	Es una bifurcación del ya mencionado Signal, permite de manera muy segura la mensajería instantánea, no ocupa un número de teléfono, tampoco una cuenta, o un usuario, lo que garantizan una conversación segura y anónima, no recopila metadatos, y es cifrado.	Se puede enviar texto y voz, imágenes y demás, se puede usar en dispositivos móviles y de escritorio, y en muy seguro y anónimo que tampoco deja huellas digitales (que se mencionó en capítulos anteriores) de nuestra navegación.
Threema	Es una aplicación de mensajería que el propio gobierno de Alemania recomienda, se centra en la seguridad y la privacidad del usuario, tanto así que no se puede sincronizar con la nube, ya que la nube no representa garantías de seguridad.	Threema es una aplicación de pago, pero de pago único, no ocupa que nos registremos o algún número de teléfono, nos asigna un id aleatorio que, si lo almacena en sus servidores, pero que no sabe a fin de cuentas quien es, garantizando que no venderá nuestros datos.
Herramientas seguras extras.		
BitLocker	Esta herramienta permite cifrar discos enteros o por partes, para el cometido, utiliza AES en modo CBC con una clave de 128 bits (funciona en Windows).	
Haveibeenpwned	Es una página web, para conocer los datos nuestros que están vulnerados, introduciendo un número de teléfono o un correo, nos otorga la información sujeta aquel correo y que está prácticamente vulnerada.	
Joindeleteme	Es una página web, que ofrece el servicio de eliminar los datos personales que las empresas, sobre todo Google, tienen de nosotros.	
Privacytools	Es una página web que facilita un compendio de herramientas para cada aspecto de nuestra privacidad en internet, ante la vigilancia que estamos sumergidos.	
Google Takeout	No hay mucho que decir, esta herramienta, propia de Google, permite solicitar los datos que la misma tiene sobre nosotros.	

MARCO METODOLÓGICO

La metodología tiene mucha relevancia, ya que describe el "cómo" se va a llevar a cabo el trabajo de investigación, las técnicas, el proceso perse. La metodología es "el conjunto de procedimientos y técnicas que se aplican de manera ordenada y sistemática en la realización de un estudio" (Coelho, 2020).

En esta investigación, se utilizó el método no experimental, ya que este método "no manipula deliberadamente las variables que busca interpretar, sino que se contenta con observar los fenómenos de su interés en su ambiente natural, para luego describirlos y analizarlos sin necesidad de emularlos en un entorno controlado" (Etecé, concepto.de, 2021).

Para la naturaleza del tema de este trabajo de investigación el método no experimental nos resultó el apropiado, ya que la observación y análisis se basan en hechos que ya tuvieron lugar, a lo que se conoce como *ex post facto*, "este tipo de investigación puede usarse para determinar las causas de un evento, a partir de sus efectos o consecuencias" (Montaño, 2021).

Además, también se utilizó el método bibliográfico, básicamente consiste en la compilación de información en base a lo que ya está publicado, para este método, es menester abundantes lecturas, además de otras fuentes, estar sumergidos en el tema en cuestión.

> La investigación bibliográfica puede definirse como cualquier investigación que requiera la recopilación de información a partir de materiales publicados. Estos materiales pueden incluir recursos más tradicionales como libros, revistas, periódicos e informes, pero también medios electrónicos como grabaciones de audio y vídeo y películas, y

recursos en línea como sitios web, blogs y bases de datos bibliográficas (Arteaga, 2020).

Finalmente, el método analítico también tuvo lugar en este trabajo, este método nos permite desglosar un todo, para así poder analizarlo, descomponerlo en sus elementos básicos y mediante el pensamiento crítico, encontrar hallazgos.

Este método se complementa muy bien con los antes mencionados, ya que nos permite, después de tener un compendio de información, analizarla, evaluarla y así, poder comprender de mejor manera el tema, desarrollar teorías, apoyar ideas, validar la hipótesis, llevar a un resultado, a una conclusión.

RESULTADOS

En este trabajo de investigación, el eje central del mismo son los datos y su protección, ya que la proliferación de la interacción de nuestras vidas con el mundo digital evoca a que cada vez más generemos más datos y muy poco se nos concientiza al respecto.

Para la recolección de datos, como mencionamos en el capítulo del marco metodológico, se utilizó el método bibliográfico, con este método, mediante la lectura de libros, artículos de periódicos, revistas y consultas web, que a pesar que no existe una enorme abundancia de información con respecto al tema planteado, encontramos información muy importante, que al utilizar también el método analítico sobre toda la recolección que nos aportó en método anterior, se pudieron determinar varios aspectos.

Con el objetivo de describir la importancia de nuestros datos históricamente, los resultados plasmaron que, desde 1804 con la era napoleónica, el recolectar datos de las personas, al ser analizados, otorga una ventaja y poder sobre los demás, así mismo, los nazis, mediante la explotación de datos, controlaban a la población, ubicar con alta efectividad a los judíos y asesinarlos, esto demuestra que nuestros datos, desde ya varios siglos atrás, son muy importantes y desde que se comenzó a recolectar, han sido muy importantes en con acontecimientos históricos, concordando con la autora (Véliz, 2021).

Con el objetivo de analizar el impacto que tienen nuestros datos en la actualidad, obtuvimos como resultados que el modelo de negocios de las grandes empresas, el cómo obtienen dinero, es a base de nuestros datos, y más aún, la venta de nuestros datos al mejor postor, el capitalismo de vigilancia y el desestabilización de democracias, además del mencionado caso de Cambridge Analytica, que explotó datos privados para beneficiar a un determinado candidato en las elecciones presidenciales de Estados Unidos, esto

evidencia que, como lo corroboran distintos autores como (Merkel, 2018), “Los datos son la materia prima del siglo XXI”.

Con el objetivo determinar alternativas de aplicaciones digitales para la protección de nuestros datos, durante el análisis de datos recopilados en esta investigación, nos dimos cuenta que los servicios más populares que usamos todo el tiempo, son inseguros en cuanto a nuestra privacidad se refiere, afortunadamente los resultados nos reflejan que existen alternativas, aplicaciones seguras, que se preocupan por nuestra privacidad, estas aplicaciones no son tan populares, pero nos protegen de que analicen cada movimiento que hacemos, cada dato que generamos a la hora de utilizar internet, y así evitar la vigilancia en la que estamos sumergidos.

DISCUSIÓN DE RESULTADOS

Es menester acentuar que lo más destacable de este caso de estudio es el manifestar el tema planteado, ya que es un tema que no es muy popular y que está directamente relacionado con las personas e influye directamente en ellas.

De acuerdo con los datos recopilados de los temas planteados y los resultados que obtuvimos, nos damos cuenta que nuestros datos han tenido valor siempre, desde la antigüedad hasta la actualidad, haciendo que la entidad que los recolecte, al analizarlos adquiera conocimiento, y el conocimiento siempre evoca al poder, y el poder siempre evoca a cometer abusos, como sucedió durante la segunda guerra mundial.

Se precisa que cada vez generamos más y más datos, cada vez estos se vuelven más importantes, tanto así que en la actualidad existen empresas gigantes que se han establecido, basando todas sus ganancias en la explotación de nuestros datos privados, lo cual, como hemos analizado, esto nos lleva a una vigilancia muy alta, el que una empresa recopile muchos datos nuestros, es considerablemente peligroso, sobre todo porque perdemos libertad, y eso nos hace vulnerables, además que perpetua el control del individuo. La explotación de datos personales en internet en nuestros tiempos contemporáneos, mediante la manipulación, ha llevado a personas a cargos gubernamentales importantes, también ha generado que la publicidad sea altamente efectiva, y demuestre injerencia al hacernos adquirir productos que no necesitamos.

Lo que nos conduce a colegir que el no generar datos, no es una opción viable, incluso, es imposible no dárselos a alguna entidad, sin embargo, lo que no es imposible es proteger nuestros datos, cuidar que información otorgamos y a quienes se la otorgamos, utilizar aplicaciones digitales que nos ayuden con la protección de nuestros datos y su privacidad, ya que las plataformas o aplicaciones muy populares que usamos a diario se

han vuelto muy nocivas con respecto a nuestros datos personales, y como hemos analizado y determinado, existen varias alternativas de aplicaciones que se preocupan por la privacidad de los datos del usuario al momento de ocupar el mundo digital.

CONCLUSIONES

Concluimos manifestando que históricamente, desde que se comenzó a recopilar datos de los ciudadanos, y descubrieron que al analizarlo podrían obtener información valiosa, los datos personales se convirtieron en una activo muy importante y quien los obtenía, también se hacía con mucho poder sobre los ciudadanos y con ello se cometieron muchos abusos.

Sobre el impacto actual de nuestros datos, los datos personales al convertirse en un activo muy importante, actualmente han pasado a convertirse en un activo muy tóxico, ya que se recopilan cantidades enormes de nuestros datos y no sabemos con exactitud para que se usan, y las ocasiones que hemos descubierto como lo han usado, han sido principalmente para manipulación y desestabilización de democracias.

En cuanto a alternativas de aplicaciones digitales, la mayor parte de empresas que ofrecen un servicio gratuito, recolectan datos de todo lo que hacemos, capitalismo de vigilancia, sin embargo, también tenemos alternativas no tan conocidas, que no recopilan datos y si lo hacen, son datos que no pueden ser explotados para luego ser vendidos, son aplicaciones que se preocupan por la privacidad del usuario y como hemos determinado, las hay para los distintos servicios que necesitemos.

RECOMENDACIONES

Ya conocemos la importancia que han tenido los datos personales en el pasado, y las atrocidades que se cometieron en nombre del poder al recolectarlas, se sugiere concientizarnos más sobre la recopilación desmedida de nuestros datos, ya que puede perpetuar el abuso de poder otra vez, si ya sucedió en el pasado, que nos garantiza que no vuelva a suceder.

También se aconseja limitar la recolección desmedida de nuestros datos personales que las plataformas y servicios digitales ejercen sobre nosotros, controlar y leer que aceptamos y que no al utilizar las mismas, moderar su uso y solicitar conocer los datos que tienen de nosotros, para generar evidencia de que nos preocupa nuestra privacidad.

Además, se sugiere tratar de no permitir la vigilancia tecnológica en la que estamos sumergidos, haciendo uso de las herramientas determinadas en este caso de estudio, herramientas que nos brindan seguridad y libertad al interactuar dentro del mundo digital, y si es posible, recomendar las mismas a más personas.

REFERENCIAS

Alpañés, E. (11 de Julio de 2021). *elpais*. Obtenido de elpais.com: https://elpais.com/ideas/2021-07-11/el-dilema-de-quedarse-en-whatsapp.html?rel=listapoyo#&rel=listaapoyo

Arteaga, G. (26 de Octubre de 2020). *testsiteforme*. Obtenido de testsiteforme.com: https://www.testsiteforme.com/investigacion-bibliografica/

Bello, E. (20 de Diciembre de 2021). *iebschool*. Obtenido de .iebschool.com/: https://www.iebschool.com/blog/data-mining-mineria-datos-big-data/

cloudflare. (s.f de s.f de s.f). *cloudflare*. Obtenido de cloudflare.com: https://www.cloudflare.com/es-es/learning/privacy/what-is-data-privacy/

Coelho, F. (26 de Octubre de 2020). *significados.com*. Obtenido de https://www.significados.com/: https://www.significados.com/metodologia-de-la-investigacion/

Economist, T. (2017). Fuel of the future. *The Economist*, 19.

Etecé, E. (31 de Agosto de 2020). *concepto.de*. Obtenido de https://concepto.de/: https://concepto.de/usufructo/

Etecé, E. (05 de Agosto de 2021). *concepto.de*. Obtenido de https://concepto.de/: https://concepto.de/investigacion-no-experimental/

Fernández, Y. (25 de Febrero de 2020). *xataka*. Obtenido de xataka.com: https://www.xataka.com/basics/que-cookies-que-tipos-hay-que-pasa-desactivas

Foer, F. (2017). *Un Mundo sin Ideas.* Barcelona: Ediciones Paidós.

Frutos, A. M. (28 de Abril de 2018). *computerhoy*. Obtenido de computerhoy.com/: https://computerhoy.com/noticias/internet/que-es-cambridge-analytica-79763

García, R. (02 de Julio de 2021). *https://www.adslzone.net/reportajes/software/que-es-brave/*. Obtenido de https://www.adslzone.net/reportajes/software/que-es-brave/: https://www.adslzone.net/reportajes/software/que-es-brave/

Gonzáles, M. (11 de Abril de 2018). *xataka.com*. Obtenido de xataka: https://www.xataka.com/legislacion-y-derechos/que-ha-pasado-con-facebook-del-caso-cambridge-analytica-al-resto-de-polemicas-mas-recientes

González, F. (09 de Mayo de 2022). *batiburrillo*. Obtenido de batiburrillo.net: https://www.batiburrillo.net/bitwarden-un-completo-gestor-de-contrasenas-de-codigo-abierto/

Harari, Y. N. (2018). *21 lecciones para el siglo XXI.* Debate.

Harari, Y. N. (2018). *21 lecciones para el siglo XXI.* Debate.

Jiménez, J. (11 de Julio de 2022). *redeszone*. Obtenido de redeszone.net: https://www.redeszone.net/tutoriales/seguridad/huella-digital-dispositivo-navegador/

José, J. S. (20 de Enero de 2021). *derechodelared*. Obtenido de derechodelared.com: https://derechodelared.com/starpage/

McAfee. (01 de Abril de 2020). *mcafee*. Obtenido de mcafee.com: https://www.mcafee.com/blogs/es-mx/privacy-identity-protection/que-es-la-privacidad-de-datos-y-como-se-puede-proteger/

Merkel, A. (24 de Enero de 2018). Foro Económico Mundial, en Davos. Davos, Suiza.

Montaño, J. (28 de Marzo de 2021). *lifeder*. Obtenido de lifeder.com: https://www.lifeder.com/investigacion-no-experimental/

Muñoz, M. Á. (19 de Diciembre de 2018). *movilzona*. Obtenido de movilzona.es: https://www.movilzona.es/2018/12/19/facebook-netflix-spotify-leer-mensajes-privados/

Orlowski, J. (Dirección). (2020). *The Social Dilemma* [Película].

Redacción. (11 de Febrero de 2021). *conceptodefinicion*. Obtenido de conceptodefinicion.de: https://conceptodefinicion.de/privacidad/

Rubio, I. (28 de Julio de 2019). *elpais*. Obtenido de elpais.com: https://elpais.com/tecnologia/2019/07/26/actualidad/1564131609_819166.html

Sánchez, J. (04 de Enero de 2019). *abc.es*. Obtenido de abc: https://www.abc.es/tecnologia/redes/abci-facebook-permitio-leer-mensajes-privados-varias-empresas-tecnologicas-como-spotify-microsoft-o-netflix-201812191022_noticia.html

Sherman, P. (03 de Mayo de 2020). *vpnoverview*. Obtenido de vpnoverview.com: https://vpnoverview.com/es/privacidad/navegacion-anonima/el-navegador-tor/

significados.com. (07 de 07 de 2022). *https://www.significados.com/*. Obtenido de significados: https://www.significados.com/datos/

Solé, R. (29 de Agosto de 2021). *profesionalreview*. Obtenido de profesionalreview.com: https://www.profesionalreview.com/2021/08/29/que-es-protonmail/

trucoslondres. (s/d de Febrero de 2020). *trucoslondres*. Obtenido de trucoslondres.com: https://trucoslondres.com/vivir/comunicacion/express-vpn/

Véliz, C. (11 de Septiembre de 2021). *https://elpais.com/*. Obtenido de elpais: https://elpais.com/ideas/2021-09-12/protejamos-nuestros-datos-no-olvidemos-como-los-usaban-los-nazis.html?event_log=oklogin

Yirda, A. (30 de Enero de 2021). *conceptodefinicion.de*. Obtenido de https://conceptodefinicion.de/: https://conceptodefinicion.de/datos/

ANEXOS

Links de las herramientas mencionadas en el último apartado (tabla 1) del marco conceptual.

Para consultas en internet:

DuckDuckGo - *https://duckduckgo.com/*

Starpage - *https://www.startpage.com/es/*

Para correo electrónico:

ProtonMail - *https://proton.me/es-es/*

Tutanota - *https://tutanota.com/es/*

Para navegar:

Brave - *https://brave.com/es/*

Tor - *https://www.torproject.org/*

LibreWolf - *https://librewolf.net/*

VPN, para proteger la conexión:

ProtonVPN - *https://protonvpn.com/es_la/*

Mullvad VPN - *https://mullvad.net/es/*

ExpressVPN - *https://www.expressvpn.com/es*

Almacenamiento en la nube:

Netxcloud - *https://nextcloud.com/*

Gestor de contraseñas:

Bitwarden - *https://bitwarden.com/*

Para autenticación:

Authy - *https://authy.com/*

Yubico - *https://www.yubico.com/?lang=es*

Microsoft Authenticator - *https://www.microsoft.com/es-es/security/mobile-authenticator-app*

Para mensajería:

Signal - *https://signal.org/es/*

Session - *https://getsession.org/*

Threema - *https://threema.ch/es*

Para cifrado de disco:

BitLocker - *https://www.m3datarecovery.com/bitlocker-windows-home/*

Adicionales para conocer qué datos nuestros están vulnerados.

Haveibeenpwned - *https://haveibeenpwned.com/*

Para borrar datos del internet.

Joindeleteme - *https://joindeleteme.com/*

Compendio de más herramientas.

Privacytools - https://www.privacytools.io/

Google Takeout - *https://takeout.google.com/settings/takeout?pli=1*

Estudio de Caso Plaza Stevven

7%

8% Texto entre comillas
5% similitudes entre comillas

< 1% Idioma no reconocido

Nombre del documento: Estudio de Caso Plaza Stevven.docx

Tamaño del documento original: 76,42 ko

Depositante: FREDY MAXIMILIANO JORDAN CORDONES

Fecha de depósito: 12/8/2022

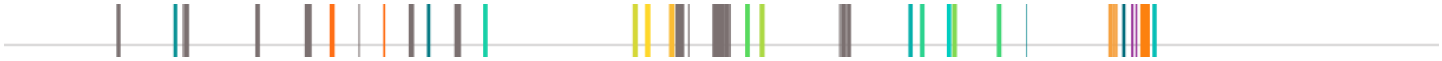
Tipo de carga: interface

fecha de fin de análisis: 12/8/2022

Número de palabras: 9466

Número de caracteres: 61.906

Ubicación de las similitudes en el documento:



Fuentes principales detectadas

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	**elpais.com** | Protección de datos: El dilema de quedarse en WhatsApp: ¿a qué renun... https://elpais.com/ideas/2021-07-11/el-dilema-de-quedarse-en-whatsapp.html?rel=listapoyo#&rel=list...	1%		Palabras idénticas: 1% (133 palabras)
2	**elpais.com** | Protejamos nuestros datos. No olvidemos cómo los usaban los nazis | Id... https://elpais.com/ideas/2021-09-12/protejamos-nuestros-datos-no-olvidemos-como-los-usaban-los-na...	1%		Palabras idénticas: 1% (140 palabras)
3	**elpais.com** | Los usuarios carecemos de garantías de la privacidad en la Red | Tecnol... https://elpais.com/tecnologia/2019/07/26/actualidad/1564131609_819166.html	< 1%		Palabras idénticas: < 1% (82 palabras)
4	**www.testsiteforme.com** | Investigación bibliográfica - Cómo llevar a cabo una - Test... https://www.testsiteforme.com/investigacion-bibliografica/	< 1%		Palabras idénticas: < 1% (57 palabras)
5	**www.movilzona.es** | Facebook ha permitido a Netflix y Spotify leer tus mensajes priv... https://www.movilzona.es/2018/12/19/facebook-netflix-spotify-leer-mensajes-privados/	< 1%		Palabras idénticas: < 1% (60 palabras)

Fuentes con similitudes fortuitas

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	**CASO DE ESTUDIO Villacis Wilman.docx** | CASO DE ESTUDIO Villacis Wilman #080a5a El documento proviene de mi biblioteca de referencias	< 1%		Palabras idénticas: < 1% (38 palabras)
2	**www.lifeder.com** | Investigación no experimental: qué es, características, ventajas, ej... https://www.lifeder.com/investigacion-no-experimental/	< 1%		Palabras idénticas: < 1% (18 palabras)

Fuentes mencionadas (sin similitudes detectadas)

Estas fuentes han sido citadas en el documento sin encontrar similitudes.

1 https://www.cloudflare.com/es-es/learning/privacy/what-is-data-privacy/

2 https://www.significados.com/

3 https://elpais.com/

4 https://elpais.com/ideas/2021-09-12/protejamos-nuestros-datos-no-olvidemos-como-los-usaban-los-nazis.html?event_log=oklogin

5 https://conceptodefinicion.de/