Revista Global de Negocios
Vol. 9, No. 1, 2021, pp. 83-93
ISSN: 2328-4641 (print)
ISSN: 2328-4668 (online)

IBFR
www.theIBFR.com

ALEXA: NECESITO PRIVACIDAD

Alicia De la Peña De León, Universidad Autónoma de Coahuila
Juan Bernardo Amezcua Núñez, Universidad Autónoma de Coahuila
Juana María Saucedo Soto, Universidad Autónoma de Coahuila
Victoria Sofía García Estrada, Universidad Autónoma de Coahuila

RESUMEN

Con el advenimiento del internet de las cosas, los hogares inteligentes son ya una realidad. Con tan sólo su voz, las personas pueden activar electrodomésticos, reproducir música, e incluso, comprar en línea. Si bien, algunos estudios previos señalan que estos equipos pueden escuchar al usuario y compartir su información con la empresa madre que los comercializa (i.e. Google, Amazon, Apple, etc.), no todas las personas conocen este dato, y al utilizar los dispositivos inteligentes pudieran estar poniendo en riesgo información confidencial. Con el objetivo conocer el comportamiento de los usuarios de bocinas inteligentes y su actitud ante el riesgo de compartir su información, se realizó un estudio exploratorio con 541 adultos mexicanos. Los resultados señalan que, si bien a los usuarios les preocupa su seguridad, y muestran una aversión al riesgo (34%), esto no los limita al momento de comprar y utilizar bocinas inteligentes. Nuestros hallazgos pueden ser de utilidad para el diseño de políticas claras en el manejo de datos personales; así como también en el lanzamiento de campañas de mercadotecnia social que tengan como meta educar a los usuarios de equipos inteligentes para que protejan su información confidencial.

PALABRAS CLAVE: Asistentes de Voz, Compras en Línea, Confianza, Estrategias de Marketing, Privacidad de Datos

ALEXA: I NEED SOME PRIVACY

ABSTRACT

With the advent of the internet of things (IoT), smart homes are now a reality. With just their voice, people can activate appliances, play music, and even shop online. Although some previous studies indicate that these devices can listen to the user and share their information with the parent company that sells them (i.e., Google, Amazon, Apple, etc.), not all people know this data, and when using their smart devices, individuals may be putting confidential information at risk. With the aim of knowing the behavior of smart speakers' users and their attitude towards the risk of sharing their information, an exploratory study was carried out with 541 Mexican adults. The results indicate that, although users are concerned about their safety, and show an aversion to risk (34%), this does not limit them when buying and using smart speakers. Our findings can be useful for the design of clear policies in the handling of personal data; as well as in the launching of social marketing campaigns with the goal to educate users of smart equipment, so they can protect their personal data.

JEL: C83, C99, D81, D83, K24, L81, M31, M39

KEYWORDS: Data Privacy, Marketing Strategies, Online Shopping, Trust, Voice Assistance Devices

INTRODUCCIÓN

Cada vez es más frecuente escuchar a las personas interactuando con distintos equipos inteligentes. Hacer llamadas telefónicas desde el auto, consultar el estado del tiempo o sintonizar una serie de televisión se ha vuelto tan simple con tan sólo decir: "Siri, llama a la oficina", "¡Ok Google, dime la temperatura!" o "Alexa, reproduce mi serie de Netflix favorita". La tecnología de reconocimiento de voz integrada a teléfonos, bocinas inteligentes y equipos de televisión permite que los usuarios interactúen fácilmente con estos equipos capaces de reconocer el lenguaje, y cuyo valor de mercado se estima tendrá un valor de 7,300 millones de dólares en 2025 (Market Research Future, 2021). De manera particular, las bocinas inteligentes o asistentes digitales funcionan mediante el uso de inteligencia artificial; y, además de procesar y comprender el lenguaje natural, pueden combinar información del usuario como sus preferencias de compra, las marcas que adquiere con mayor frecuencia, su ubicación, así como algunos hábitos (como, por ejemplo, música y series de televisión preferidas) para crear, mediante algoritmos modelos y patrones de comportamiento (Oracle, 2021).

Si bien los dispositivos más populares para usar asistentes de voz son actualmente los *smartphones* y las bocinas inteligentes, ya existen en el mercado electrodoésticos, televisiones inteligentes, juguetes y automóviles que no sólo responden a la voz de sus dueños (Petrock, 2020), sino que además llevan un registro de las interacciones con las personas, y comparten información con las empresas madre que los crearon (i.e. Google, Apple, Amazon, Samsung, etc.). Aunque el objetivo principal de recabar los datos personales de los usuarios es mejorar la experiencia de uso y corregir fallas; éste representa un riesgo para la privacidad de los consumidores (Vimalkumar et al., 2021).

Con el objetivo de examinar la percepción que tienen los consumidores sobre los riesgos de seguridad al utilizar asistentes de voz, y el nivel de confianza que tienen en dichos equipos realizamos una investigación exploratoria con hombres y mujeres adultos del norte de México. A continuación, presentamos en la primera sección una revisión de literatura referente al riesgo en el uso de tecnologías digitales. En seguida, presentamos la metodología del estudio, y continuamos con la presentación de resultados en la tercera sección. Finalmente, en la última sección presentamos nuestras conclusiones, nuestras propuestas para la realización de estudios futuros y las limitaciones que observamos al realizar la investigación.

REVISIÓN DE LITERATURA

Los avances tecnológicos han permitido que los individuos sean más productivos tanto en sus empleos, como en su hogar, y alcancen mejores niveles de bienestar. Desde que los llamados productos "inteligentes" llegaron al mercado podemos observar personas que aprovechan estos pequeños dispositivos para monitorear su salud, medir los kilómetros recorridos al salir a correr, calcular las calorías que contienen sus pequeños gustos culposos, e inclusive resurtir su alacena, limpiar la sala, sintonizar su música preferida, o crear el ambiente apropiado en su habitación para una noche romántica o un momento de meditación. Y aunque parecen actividades complejas, muchas se realizan con pequeñas bocinas inteligentes o asistentes de voz, capaces de ejecutar distintas tareas al ser activadas con la voz de sus dueños (Hoy, 2018; Perry, 2017; Reportlinker, 2017).

Los Asistentes Virtuales Personales (AVP o VPA por sus siglas en inglés), o bocinas inteligentes como comúnmente se les conocen, son equipos pequeños, conectados a internet, que pueden escuchar la voz del usuario y responder a distintos comandos, sin que la persona se mueva de su lugar (Hoy, 2018; Kowalczuk, 2018). Los AVP están vinculados a distintas aplicaciones -también llamados *skills*-, por lo que los usuarios pueden fácilmente accesar a su cuenta de Spotify para escuchar música, conocer las últimas noticias, encender la calefacción en una habitación, ordenar a la aspiradora que limpie la cocina, hacer compras en Amazon e incluso, reproducir series de Netflix. Además, se convierten en eficientes asistentes, al programar agendas, fijar recordatorios, activar alarmas e inclusive, pueden hacer cálculos matemáticos (Hoy, 2018).

Estos asistentes virtuales son distintos a otros dispositivos tecnológicos, ya que son capaces de emular rasgos humanos al conversar con el usuario en su propio idioma; suelen ser muy fáciles de operar, ya responden rápidamente a comandos de voz y no requieren manipulación directa con las manos, lo que permite que los usuarios los utilicen mientras realizan otra tarea, o incluso, mientras conducen su coche; cuando la conexión a internet es apropiada, suelen ser muy eficientes al brindar la información que el usuario solicita; y aunque pudiera ser una ventaja, siempre están escuchando e incluso observando lo que las personas hablan y hacen a su alrededor (Vimalkumar et al., 2021).

En el ámbito del marketing, los AVP se han convertido en un punto de contacto más para las marcas, ya que éstas se han dado a la tarea de crear aplicaciones específicas que al ser activadas con la voz del usuario le permiten interactuar directamente con una empresa y sus productos (Smith, 2020). Estas aplicaciones reciben distintos nombres: Amazon les llama *Skills* y Google les llama *Actions*. A través de ellas, se genera un vínculo entre el consumidor y la marca, pues éste puede comprar flores, ordenar pizzas, o buscar recetas para cocinar platillos con sus marcas preferidas (Smith, 2020).

AVP: Herramientas Para Acompañar, Informar y Entretener

Estudios previos basados en la Teoría de Usos y Gratificaciones identifican cuatro razones principales para utilizar AVP: interacción virtual para escapar de la realidad; aprendizaje e información; juego y relajación; y, búsqueda de solución de problemas (Lee & Cho, 2020). Y si bien las bocinas inteligentes tienen muchas funciones, sus usos principales están vinculados al entretenimiento: escuchar música o podcasts, ver series de televisión o videos cortos de YouTube son algunas de las actividades que los usuarios realizan ayudados de Alexa, Siri o Google (Ashfaq, Yun & Yu, 2020; Reportlinker, 2017; Statista, 2021). Escuchar noticias y pedir información sobre el tráfico o el clima, también son acciones comunes de los usuarios de AVPs (Smith, 2020). Para pasar un buen rato, los usuarios pueden pedir a su AVP que les cuente un chiste o una historia; o bien, pueden jugar trivias y adivinanzas (Hoy, 2018).

Sin embargo, con la llegada del COVID-19 y el obligatorio encierro, para muchas personas, los AVP se convirtieron también en compañeros de casa (Statista, 2021). Empresas como la galletera Moonpie en Estados Unidos, se dieron a la tarea de diseñar *skills* (programas interactivos) de Alexa, para brindar a los usuarios una herramienta de conversación y entretenimiento, y combatir así la soledad, el aburrimiento y la tristeza generados por el aislamiento social (Schwartz, 2020). En el tema de la salud, algunas instituciones como la Clínica Mayo, crearon *skills* para orientar a los individuos en temas de la pandemia, e incluso aconsejar para atender pequeñas emergencias caseras con consejos de primeros auxilios para quienes se encontraban enfermos en sus hogares (Mayo Clinic, 2020).

En algunos países, como Israel, India y Reino Unido, se aprovecharon los dispositivos inteligentes para monitorear la ubicación y los movimientos de los ciudadanos, y utilizar dichos datos en programas preventivos para reducir los contagios del virus; así como para asegurarse de que los individuos estaban cumpliendo con las restricciones de distanciamiento social (Brough & Martin, 2021). Y si bien en países como China, los ciudadanos están acostumbrados a ser vigilados por las autoridades de su país, en otras regiones del mundo, las personas son más cautelosas con la información que comparten a través de la tecnología digital. Al buscar medidas de protección sanitaria, surgen entonces nuevos retos: ¿qué tanta información debe compartir el usuario con sus equipos inteligentes para prevenir un contagio de COVID-19 sin poner en riesgo su seguridad y privacidad? ¿Cómo será el consumidor post-COVID-19? ¿Sacrificará su privacidad a cambio de recibir los beneficios de realizar actividades en el entorno virtual? (Brough & Martin, 2021).

Privacidad y Seguridad

Con la llegada de los dispositivos inteligentes surgen varias oportunidades para las empresas. Por un lado, al ofrecer a los usuarios avanzados dispositivos tecnológicos logran diferenciarse de la competencia, a la vez que brindan beneficios a los compradores, quienes buscan al adquirir estos objetos, simplificar diferentes actividades cotidianas; por otro lado, tienen la posibilidad de obtener información de primera mano, ya que cada vez que el consumidor utiliza un reloj inteligente, un robot de limpieza o un asisstente de voz está compartiendo datos con los creadores de dichos dispositivos. Y si bien algunas marcas son muy transparentes en relación a sus prácticas de manejo de datos, otras prefieren mantener un secretismo y se dan a la tarea de controlar la información que el usuario comparte con ellas (Morey, Forbath & Schoop, 2015).

¿Qué tipo de datos almacenan y utilizan las marcas? Principalmente se identifican tres categorías: 1. Datos autoreportados (i.e., información que el usuario da de forma voluntaria, como su correo electrónico, o lugar de trabajo); 2. Huellas Digitales o datos creados de manera digital (p.ej., el historial de búsqueda que se va creando y almacenando cuando una persona visita un sitio de internet); y 3. Datos de segmentación (i.e., perfiles creados por las marcas tras analizar los datos y huellas digitales que dejan los usuarios, y que permiten predecir sus intereses y comportamientos de compra) [Morey et al., 2015].

Los creadores de los AVP señalan, que el hecho de que los equipos almacenen datos y huellas digitales de las personas que interactúan con estos dispositivos, tiene como meta aprender del usuario, para corregir fallas en los equipos y diseñar así mejores versiones de los mismos (Conger, Pratt & Loch, 2013; Malkin et al., 2019). Sin embargo, algunos usuarios no leen todas las indicaciones al momento de instalar los dispositivos, por lo que quizás estén aceptando que su información no sólo sea almacenada por los fabricantes del equipo, sino que ésta se llegue a compartir con terceros, lo cual pone en riesgo su privacidad y seguridad (Bélanger & Crossler, 2011; Lau, Zimmerman & Schaub, 2018).

Desde niños, las personas aprenden a resguardar su intimidad y proteger sus bienes, partiendo desde el espacio físico y elementos visibles del ambiente: cierran las cortinas de su habitación por la noche, ponen candado en las puertas, o evitan conversaciones delicadas cerca de personas extrañas (Schomakers, Lidynia & Ziefle, 2020). Pero ¿qué pasa en la interacción con equipos digitales y entornos virtuales? ¿Aplican los conceptos de cortinas, candados y cerrojos? Si bien cierta información se puede proteger con el uso de contraseñas y códigos especiales, en el entorno digital los riesgos de ser observados suelen no ser tan perceptibles, además, muchos individuos no están conscientes del riesgo que representa compartir su información; y otros, consideran que la protección activa de su información es demasiado compleja y poco factible, por lo que se han resignado a compartirla de manera continua (Hoffmann, Lutz & Ranzini, 2016; Schomakers et al., 2020).

Los AVP son tan versátiles, que las personas incluso tienen más de una bocina en su hogar, convirtiendo así a estos pequeños equipos en parte del mobiliario, por lo que es común que los usuarios se olviden de que existe la posibilidad de que éstos utilicen sus datos personales de manera poco ética. Es tanta la interaccion que puede darse entre el usuario y el AVP, que poco a poco se va generando una relación de confianza entre el consumidor y el equipo, quien descarga ciertas responsabilidades en el AVP, como por ejemplo el programar el encendido de luces al anocher, activar una alarma por las mañanas, poner a trabajar al robot de limpieza, etc. (Foehr & Germelmann, 2020), esperando que éstas se realicen de manera puntual… y confidencial. De hecho, estudios previos sugieren que los usuarios asignan una serie de cualidades humanas a sus equipos, lo que les da un aura de confianza (Ewers, Baier, & Höhn, 2020; Foehr & Germelmann, 2020), olvidando que las bocinas inteligentes tienen la capacidad de almacenar conversaciones y videos de todas las actividades que sus dueños realizan cerca de ellos (Malkin et al., 2019).

Sin embargo, dado que los AVP ofrecen a los usuarios funciones y aplicaciones que les simplifican la vida, e incrementan su comodiad y la conveniencia de uso, un porcentaje importante de consumidores acepta que las marcas utilicen sus datos y huellas digitales, para lograr así las ventajas de un mejor desempeño con sus equipos (Morey et al., 2015). Lo anterior, nos lleva a preguntarnos: ¿qué uso le da el adulto mexicano a los AVP? ¿le preocupa su privacidad? ¿verifica las políticas sobre la información que comparte con estos equipos? ¿qué riesgos percibe al utilizar bocinas inteligentes? Con el objetivo de dar respuesta a estas preguntas realizamos una investigación exploratoria y descriptiva, cuya metodología se describe a continuación.

METODOLOGÍA

El objetivo de esta investigación es identificar la actitud del adulto mexicano hacia los riesgos de privacidad que representa el usar asistentes de voz o bocinas inteligentes. Para dar respuesta a este objetivo, se diseño una investigación cuantitativa utilizando la escala de actitud ante la privacidad de Buchanan et al., (2007) y la escala de divulgación de identidad desarrollada por Stutzman (2006), para primero, poder identificar a los consumidores que actualmente cuentan con un asistente de voz, y posteriormente analizar los riesgos que perciben al utilizar dichos asistentes de voz para realizar distintas actividades en sus hogares y/o centros de trabajo. En el diseño de cuestionario se utilizaron preguntas dicotómicas (respuesta Si y No) y de escala de Likert de 5 puntos.

Para distribuir el cuestionario y realizar el trabajo de campo, se utilizo la plataforma digital *Survey Monkey,* la cual permite aplicar cuestionarios enviando un enlace por correo electrónico o a través de redes sociales como Whatsapp. Dado que este estudio se realizó durante la pandemia por el COVID-19 el trabajo de campo se llevó a cabo de manera remota. La selección de la muestra se realizó con adultos mexicanos mayores de 18 años. El levantamiento de información se realizó en un periodo de tres semanas en el invierno de 2021 en una ciudad del norte de México. Una vez finalizado la aplicación de encuestas, los datos se analizaron mediante el paquete estadístico SPSS utilizando modelos de regresión para analizar el comportamiento de los usuarios de asistentes de voz.

RESULTADOS

Con la llegada de los nuevos reglamentos relacionados con el manejo de datos personales, a países como México, el analizar la percepción que tienen los consumidores del riesgo que implica el compartir su información personal ha cobrado mayor importancia. Nuestra investigación aporta hallazgos interesantes sobre la dualidad en el comportamiento de los individuos; quienes por un lado afirman ser aversos al riesgo, y por otro, al momento de visitar diferentes páginas de internet o utilizar dispositivos inteligentes ignoran los riesgos de compartir sus datos, buscando la comodidad y facilidad de uso, o simplemente toman decisiones con base en heurísitcas que simplifican el proceso. Estos hallazgos se presentan en las siguientes secciones.

Estadísticas Descriptivas

En el estudio participaron 541 adultos (59% mujeres) en un rango de edad de los 18 a 55 años, lo cual nos permitió estudiar el comportamiento de los usuarios de asistentes de voz en distintas etapas de su ciclo de vida. 46.6% de los entrevistados son estudiantes universitarios; 25% estudia y trabaja; y 23.3 % de los participantes corresponde a empleados y 5.2% son desempleados.

Al preguntar sobre sus hábitos en redes sociales, observamos que, entre los participantes en el estudio, el 93% utiliza Facebook, 78.7% utiliza Instagram, 97.2% se comunica a través de Whatsapp y el 49.4% utiliza TikTok. Para accesar a sus redes sociales o bien, configurar una nueva cuenta en un sitio de internet, el 21.6% utiliza su número telefónico; 36.6%, su correo electrónico; y 31.1%. accesa a distintas redes sociales

con su perfil de Facebook, permitiendo entonces que tanto Facebook como la nueva red social visitada tengan acceso a información del usuario y puedan rastrear sus actividades digitales.

Al momento de preguntar si poseen un asistente digital, únicamente el 37% de los entrevistados cuenta con un AVP; destacando el uso de Siri (22.7%), Google Assistant (17.9%), Alexa 14%) y Google Home (5.5%); para actividades tan variadas como lo son escuchar música (28.5%), pedir información (30.9%), administrar la agenda personal (7.0 %), controlar otros equipos en casa u oficina (8.3%), encender/apagar luces (5.5%), e incluso, hacer llamadas telefónicas (18.1%). La Tabla 1 presenta un resumen de las características de los participantes en el estudio y sus comportamientos habituales al utilizar asistentes de voz.

Tabla 1: Rasgos del Usuario de Asistentes de Voz en México

Atributo		**%**
Género		
	Femenino	59.0
	Masculino	41.0
Ocupación		
	Estudiante universitario	46.6
	Estudia y trabaja	25.0
	Empleados	23.3
Hábitos digitales		
	Utiliza Facebook	93.0
	Utiliza Instagram	78.7
	Se comunica por Whatsapp	97.2
	Ve videos en TikTok	49.5
	Utiliza asistentes de voz	37.0

En esta Tabla 1 se presenta el perfil general de los participantes en el estudio, lo cual nos permite analizar el comportamiento de los usuarios de asistentes de voz y su percepción de los niveles de seguridad que éstos ofrecen.

Actitud Hacia el Riesgo

Tras haber analizado el perfil de los participantes, se utilizó el paquete estadístico SPSS para calcular el índice de aversión al riesgo de los participantes, utilizando 7 ítems. El índice obtenido es de 3.73; es decir en promedio los entrevistados prefieren evitar situaciones de riesgo, que comprometan la integridad de sus datos. Al analizar la relación entre edad, género, ocupación y nivel de estudios y la percepción de riesgo al utilizar bocinas inteligentes, encontramos una relación significativa en las variables género y edad (β: 2.945, p=0.000). Descubrimos que el 28.5% de los hombres se consideran arriesgados, en tanto que sólo el 19.75% de las mujeres se percibe como tal. En cuanto a la edad, los jóvenes menores de 25 años son quienes se declaran como los más arriesgados.

Adicionalmente, los hallazgos señalan que un 28.3% de los participantes considera que las empresas pueden espiarlos a través de los asistentes de voz; y, por lo tanto, sólo un 10.2% se siente seguro comprando a través de estos dispositivos. El 71.7% considera que los asistentes digitales utilizan su información confidencial, particularmente para hacerles llegar mensajes publicitarios personalizados (40.5%); y el 48.1% está convencido de que las marcas recaban datos personales de manera furtiva para ser utilizados por las propias empresas. Sin embargo, están dispuestos a aceptar ya que el 46.4% considera que recibirá un beneficio por compartir sus datos; y el 43.3% se declara ser una persona que controla el tipo y la cantidad de información que comparte con las empresas.

Es importante señalar, que si bien el 78.7% afirma conocer los riesgos que representa compartir sus datos personales al utilizar internet, redes sociales o dispositivos digitales; el 49.1% ha compartido su correo electrónico; el 87.8% comparte su fecha de cumpleaños; el 47.3% ha compartido su número telefónico; e incluso información sobre sus cuentas bancarias (7.6%). Adicionalmente, son personas que acostumbran a

subir su fotografía en el perfil de redes sociales (48%); el 34% hace check-in (i.e., notifican a su red de seguidores cuando llegan a algún lugar); y el 71.9% comparte las fotografías de los lugares que visita. Estudios previos señalan, que este tipo de datos -que por cierto se comparten de manera voluntaria-, pueden ser utilizados por ciberdelincuentes para cometer distintos tipos de delito (Rossi & Musolesi, 2014); sin embargo, pareciera que las personas no consideran este riesgo al momento de exponer su información y detalles de su vida privada en las redes sociales.

CONCLUSIONES

Los resultados de esta investigación nos permiten entender el comportamiento de las personas que utilizan asistentes virtuales y/o bocinas inteligentes y la influencia que tiene su actitud hacia el riesgo al momento de utilizarlos. Nuestros hallazgos identifican actitudes y comportamientos interesantes, que contribuyen a enriquecer la teoría de usos y gratificaciones, agregando un elemento importante: el riesgo que representa utilizar los AVP. De acuerdo con nuestros entrevistados, los asistentes virtuales favorecen la realización de infinidad de tareas en casa y oficina, tanto de esparcimiento como de simplificación de tareas, pues se pueden utilizar tanto para escuchar música y pasar un buen rato, mantenerse informado con las últimas noticias, activar robots de limpieza, vigilar el hogar, encender y apagar sistemas eléctricos y de seguridad, e incluso, dictar textos a programas como Word, entre otras actividades.

Esta investigación así mismo, contribuye a la teoría de motivación de protección (Protection Motivation Theory o PMT) de Rogers & Prentice-Dunn (1997), al identificar la dualidad que existe en las decisiones del consumidor, y al sugerir el papel que juega la comodidad en el contexto de la privacidad de información. Al buscar inmediatez y simplificación de actividades cotidianas, los usuarios de AVP descuidan algunos aspectos de seguridad personal, dejando de lado el riesgo de compartir sus rutinas diarias con estos equipos inteligentes a cambio de obtener entretenimiento e información de manera rápida.

Aún cuando en México el costo de los AVP no los hace asequibles para toda la población, el incremento en la demanda de estos equipos, así como el surgimiento de distintas marcas en el mercado hace que cada vez sean más las personas interesadas en adquirirlos, ya que no sólo son un objeto tecnológico de moda, sino que, además, simplifican distintas actividades y tareas. A medida que las personas (y también las empresas y organizaciones) descubren sus ventajas, surgen nuevas aplicaciones y usos, convirtiendo a estos pequeños equipos en verdaderos asistentes digitales. Sin embargo, es importante notar que con la llegada de las llamadas bocinas inteligentes a hogares y oficinas surgen nuevos retos: no sólo el consumidor debe aprender a configurarlos para poder interactuar con ellos, sino que además tendrá que estar atento a la información que comparte con ellos, y el uso que les da cada integrante de la familia.

Las empresas que fabrican los asistentes los han configurado para que sean equipos inteligentes, que documente información del usuario, tanto para innovar con nuevos productos, como para conocer patrones de comportamiento y hábitos de compra, lo cual se traduce en el lanzamiento de nuevos servicios, equipos más avanzados y campañas publicitarias personalizadas.

Desafortunadamente, existe el riesgo de los ciber delincuentes, quienes pueden en dado caso crear aplicaciones falsas para usarse con estos equipos y obtener así, datos importantes de los usuarios, que posteriormente pudieran traducirse en robos y suplantaciones de identidad.

Nuestros hallazgos sugieren que, si bien las personas están conscientes de los riesgos que representa utilizar estos equipos, el valor que perciben es mayor, por lo que la novedad, la practicidad y la comodidad de uso superan el miedo a ser vigilados por las empresas, o a ser víctimas de los ciber delincuentes, por lo que requieren apoyo y orientación para tomar decisiones racionales enfocadas a prevenir delitos cibernéticos.

Esto da pie para crear campañas de educación claras, que expliquen a los usuarios de asistentes digitales los riesgos que corren al utilizarlos y compartir de manera poco cuidadosa sus datos. Estas campañas, además, deberán proporcionar una guía para que los usuarios configuren sus dispositivos de modo tal que sus datos personales y financieros queden protegidos. De igual manera, organismos públicos deberán crear reglamentos y normas claras para el manejo seguro de los datos que los usuarios comparten en este tipo de equipos, ya que desafortunadamente existen aún lagunas legales que deben ser atendidas con prontitud por parte de las autoridades.

Podemos decir que al entender cuándo, cómo y porqué las personas utilizan asistentes de voz, aún y cuando estén poniendo en riesgo su privacidad y seguridad personal; estaremos en posibilidad de diseñar estrategias de mercadotecnia adecuadas para brindar al consumidor nuevas experiencias de consumo, y también garantizar condiciones de uso seguro.

Limitaciones del Estudio y Estudios a Futuro

Aún y cuando los AVP o bocinas inteligentes están al alcance de todos aquellos adultos mexicanos con capacidad de compra, esta investigación se realizó únicamente con consumidores del norte de México; por lo que la segunda etapa del estudio puede implementarse en otras regiones del país.

La segunda limitación se basa en las características de la muestra, la cual estuvo integrada principalmente por estudiantes universitarios, ejecutivos y profesionistas. Con el fin de comparar las actitudes y percepciones de un grupo demográfico distinto se puede realizar una investigación con niños y/o adultos mayores. Esto permitirá generar información útil para que los creadores y comercializadores de equipos inteligentes puedan atender diferentes segmentos de mercado, y diseñar las aplicaciones apropiadas.

No debemos olvidar a los adoptadores tardíos de tecnología, quienes eventualmente pueden llegar a convertirse en un importante segmento de mercado si logramos identificar claramente las razones por las cuales aún no cuentan con un AVP. Dado que en México el porcentaje de adultos mayores que utiliza bocinas inteligentes es todavía muy bajo (20% de acuerdo con Voicebot, 2020), propones utilizar el Modelo de Aceptación Tecnológica de Venkatesh & Davis (1996), para identificar su actitud ante las bocinas inteligentes y la percepción que tienen de la seguridad de su información al utilizarlas.

Es importante también investigar el uso que se le pueden dar a estos dispositivos inteligentes para atender a personas convalecientes en casa u hospital, invidentes o incluso, personas con alguna discapacidad motriz, que les impida utilizar el teclado de una computadora o teléfono celular; así como los retos en seguridad y privacidad que implicaría el adoptar estas tecnologías en el ámbito del cuidado de la salud.

Finalmente, desde el punto de vista de marketing, se puede analizar qué marcas han diseñado *skills* específicos para los asistentes de voz disponibles en el mercado (p.ej. Levi´s, MoonPie, Purina, Starbucks, etc.), la percepción que tiene el consumidor de dichos *skills*, y su disposición a compartir su información a cambio de utilizarlos de manera gratuita.

No podemos negar que los equipos inteligentes llegaron para quedarse en los hogares y oficinas, por lo que conocer su potencial de mercado y los posibles riesgos que su uso representa es una tarea importante para quienes realizamos estudios de comportamiento del consumidor.

REFERENCIAS

Ashfaq, M., Yun, J., & Yu, S. (2020). My Smart Speaker is Cool! Perceived Coolness, Perceived Values, and Users' Attitude toward Smart Speakers. *International Journal of Human–Computer Interaction*, 1-14.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. *MIS Quarterly*, *35*(4), 1017-1041.

Brough, A. R., & Martin, K. D. (2021). Consumer privacy during (and after) the COVID-19 pandemic. *Journal of Public Policy & Marketing*, *40*(1), 108-110.

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U. D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American society for information science and technology*, *58*(2), 157-165.

Conger, S., Pratt, J. H., & Loch, K. D. (2013). Personal information privacy and emerging technologies. *Information Systems Journal*, *23*(5), 401-417.

Ewers, K., Baier, D., & Höhn, N. (2020). Siri, do i like you? Digital voice assistants and their acceptance by consumers. *Special Issue on Artificial Intelligence and Robots in Service Interaction, in Journal of Service Management Research, 4*(1), 52-66.

Foehr, J., & Germelmann, C. C. (2020). Alexa, can I trust you? Exploring consumer paths to trust in smart voice-interaction technologies. *Journal of the Association for Consumer Research*, *5*(2), 181-205.

Hoffmann, C. P., Lutz, C., & Ranzini, G. (2016). Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *10*(4), 1-18.

Hoy, M. B. (2018). Alexa, Siri, Cortana, and more: an introduction to voice assistants. *Medical reference services quarterly*, *37*(1), 81-88.

Kowalczuk, P. (2018). Consumer acceptance of smart speakers: a mixed methods approach. *Journal of Research in Interactive Marketing*, *12*(4), 418-431.

Lau, J., Zimmerman, B., & Schaub, F. (2018). Alexa, are you listening? privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. *Proceedings of the ACM on Human-Computer Interaction*, *2*(CSCW), 1-31.

Lee, H., & Cho, C. H. (2020). Uses and gratifications of smart speakers: Modelling the effectiveness of smart speaker advertising. *International Journal of Advertising*, *39*(7), 1150-1171.

Malkin, N., Deatrick, J., Tong, A., Wijesekera, P., Egelman, S., & Wagner, D. (2019). Privacy attitudes of smart speaker users. *Proceedings on Privacy Enhancing Technologies*, *2019*(4), 250-271.

Market Research Future (2021). Global Voice Assistant Market. https://www.marketresearchfuture.com/reports/voice-assistant-market-4003

Mayo Clinic (2020). Skills from Mayo Clinic. https://www.mayoclinic.org/voice/apps

Morey, T., Forbath, T., & Schoop, A. (2015). Customer data: Designing for transparency and trust. *Harvard Business Review*, *93*(5), 96-105.

Oracle (2021). ¿Qué es un asistente digital? https://www.oracle.com/mx/chatbots/what-is-a-digital-assistant/

Perry, J. (2017). Shopping With Alexa. Wunderman Thompson. https://intelligence.wundermanthompson.com/2017/03/study-shopping-alexa/

Petrock, V. (2020). Voice Assistant and Smart Speaker Users 2020. *eMarketer.* https://www.emarketer.com/content/voice-assistant-and-smart-speaker-users-2020

Reportlinker Insight (2017). "Alexa, Please Turn on the Lights at 7 pm:" Smart Automation Comes Home. https://www.reportlinker.com/insight/smart-automation-comes-home.html

Rogers, R. W., & Prentice-Dunn, S. (1997). Protection motivation theory. In D. S. Gochman (Ed.), *Handbook of health behavior research 1: Personal and social determinants* (pp. 113–132). Plenum Press.

Rossi, L., & Musolesi, M. (2014, October). It's the way you check-in: identifying users in location-based social networks. *Proceedings of the second ACM conference on Online social networks, 10*(1), 215-226.

Schwartz, E.H. (2020). "New MoonPie MoonMate Alexa Skill Makes a Snack Cake Your Virtual Roomate". *Voicebot.ai.* https://voicebot.ai/2020/05/07/new-moonpie-moonmate-alexa-skill-makes-a-snack-cake-your-virtual-roommate/

Schomakers, E. M., Lidynia, C., & Ziefle, M. (2020). All of me? Users' preferences for privacy-preserving data markets and the importance of anonymity. *Electronic Markets*, *30*(3), 649-665.

Smith, K. T. (2020). Marketing via smart speakers: what should Alexa say?. *Journal of Strategic Marketing*, *28*(4), 350-365.

Statista (2021). Listening to news on Smart speakers during coronavirus. https://www.statista.com/statistics/1117925/listening-to-news-on-smart-speakers-after-covid-19-outbreak-in-the-us-by-age/

Stutzman, F. (2006). An evaluation of identity-sharing behavior in social network communities. *Journal of the International Digital Media and Arts Association*, *3*(1), 10-18.

Venkatesh, V., & Davis, F. D. (1996). A model of the antecedents of perceived ease of use: Development and test. *Decision sciences*, *27*(3), 451-481.

Vimalkumar, M., Sharma, S. K., Singh, J. B., & Dwivedi, Y. K. (2021). 'Okay Google, What About My Privacy?': User's Privacy Perceptions and Acceptance of Voice Based Digital Assistants. *Computers in Human Behavior*, *120*(6), 106-123.

Voicebot (2020). Voice Assistant Demographic Data -Young Consumers More Likely to Own Smart Speakers while Over 60 Bias Toward Alexa and Siri. https://voicebot.ai/2019/06/21/voice-assistant-demographic-data-young-consumers-more-likely-to-own-smart-speakers-while-over-60-bias-toward-alexa-and-siri/

BIOGRAFÍA

Alicia De la Peña es doctora en Ciencias Administrativas, con especialidad en comportamiento del consumidor y responsabilidad social corporativa por la EGADE Business School. Es profesora investigadora de la Universidad Autónoma de Coahuila. Integrante del Cuerpo Académico de Administración de la Mercadotecnia. Es miembro del Sistema Nacional de Investigadores, Nivel Uno.

Bernardo Amezcua es doctor en Ciencias Administrativas, con especialidad en comportamiento del consumidor y responsabilidad social corporativa por la EGADE Business School. Es profesor investigador de la Universidad Autónoma de Coahuila. Forma parte del Cuerpo Académico de Administración de la Mercadotecnia. Es miembro del Sistema Nacional de Investigadores, Nivel Uno.

Juana María Saucedo Soto. Doctora en Administración y Dirección de Empresas por la Universidad Politécnica de Catalunya, Catedrático Investigador de Tiempo Completo. Responsable del Cuerpo Académico Administración de la Mercadotecnia. Se puede contactar en la Facultad de Mercadotecnia de la Universidad Autónoma de Coahuila. Es miembro del Sistema Nacional de Investigadores, Nivel Candidato.

Victoria Sofía García Estrada es estudiante de Octavo Semestre de la Licenciatura en Mercadotecnia (Matrícula 15608231). Participa en el diseño e implementación de proyectos de investigación enfocados a estudiar el comportamiento del consumidor en temas de comercio electrónico y uso de tecnologías digitales.