Universidad del País Vasco Euskal Herriko Unibertsitatea

EKONOMIA ETA ENPRESA FAKULTATEA
FACULTAD DE ECONOMÍA Y EMPRESA

EKONOMIA ETA ENPRESA ZIENTZIEN FAKULTATEA
FACULTAD DE CIENCIAS ECONÓMICAS Y EMPRESARIALES

GRADO EN MARKETING

Curso 2023/2024

La Revolución Digital y La Privacidad Del Consumidor

Autor: Adrián Plaza Iglesias

Director: Lorenzo Vicario Martinez

En Bilbao, a 27 de Septiembre de 2024

Resumen

El objetivo de este Trabajo de Fin de Grado es analizar la situación actual de la privacidad de los consumidores en esta era digital en la que vivimos. Cada vez que nos registramos en una página web, compramos un artículo por internet o simplemente navegamos por internet dejamos una huella digital imperecedera de alto valor comercial.

Nuestros datos son algo muy valioso para las empresas, por lo que están dispuestas a pagar grandes sumas de dinero por ese tipo de información y a adquirirla incluso de manera ilícita o poco ética. Su alto valor no les da el derecho de lucrarse a costa de nuestra privacidad.

Las estrategias utilizadas en el marketing comercial son las mismas que las usadas en el marketing político, pero el objetivo de este último es completamente distinto.

Nuestra información es algo muy importante y el consumidor debe ser consciente del tipo de información está dejando en internet. Las empresas y organizaciones, por su parte, tienen el deber de salvaguardar correctamente esta información y no lucrarse de ella, al menos sin el consentimiento informado del consumidor. Todo debe ir acompañado de una correcta regulación legal.

Palabras clave: privacidad, era digital, estrategias de marketing, regulación

Summary

The objective of this Final Degree Project is to analyse the state of consumer privacy in the current digital era. Every time we register on a website, make an online purchase, or simply browse the internet, we leave behind a long-lasting digital footprint with significant commercial value.

Our data is highly valuable to companies, which is why they are often willing to pay large sums for it, sometimes even acquiring it through illicit or unethical means. However, the value of this information does not grant them the right to profit at the expense of our privacy.

The strategies used in commercial marketing are the same as those used in political marketing, but the objective of the latter is completely different.

Personal information is crucial, and consumers should be aware of what data they are leaving behind online. Companies and organisations, in turn, have a responsibility to

safeguard this data properly and not exploit it without the consumer's informed consent. Furthermore, this process must be supported by appropriate legal regulations.

Keywords: privacy, digital age, marketing strategies, regulation

Índice

1. Introducción **5**

2. Objetivos **7**

3. Metodología **8**

4. La Revolución Digital y la Sociedad Digital **9**

5. La Revolución Digital: marketing y consumidores **12**

5.1. Oportunidades y riesgos 17

5.1.1. Oportunidades 17

5.1.2. Riesgos 20

6. El marketing y la privacidad del consumidor **26**

6.1. El marketing comercial y la privacidad del consumidor: 31

6.1.1. Pedir permiso para espiar 31

6.1.2. Comodidad en casa pagada con tu privacidad 36

6.1.3. Demanda a Apple 41

6.2. El marketing político y la privacidad del ciudadano: 43

6.2.1. Política personalizada 43

6.2.2. Facebook decide a quién debes votar 47

6.2.3. Google frente al Reglamento Europeo 50

6.2.4. Tus datos a cambio de un billete de lotería 54

7. Conclusiones **58**

8. Bibliografía **61**

Índice de figuras

Figura 1: Reseña de Google 13

Figura 2: Enlace a redes sociales 15

Figura 3: Gráfico de respuesta de usuarios al ATT por país. Mayo 2021 33

Figura 4: Inversión publicitaria por meses en Android y Apple 34

Figura 5: Familia Alexa 36

Figura 6: Los algoritmos de Movimiento Inteligente de Astro construyen un mapa de profundidad del entorno en el que se mueve 39

1. Introducción

Este Trabajo de Fin de Grado se centra en la privacidad de los consumidores en internet. Escogí este tema después de escuchar cómo personas cercanas a mí habían recibido cargos fraudulentos en sus tarjetas de crédito tras realizar compras en páginas web. Al principio pensé: “Habrán introducido su tarjeta de crédito en alguna página poco fiable”; sin embargo, unos días después, yo mismo me encontré con cargos fraudulentos en mi tarjeta de crédito. Me considero una persona bastante cautelosa con los datos sensibles y utilizo métodos de pago seguros, como PayPal y PaySafeCard, siempre que es posible. Este suceso me hizo darme cuenta de la importancia de nuestra privacidad como consumidores y me motivó a investigar más sobre el tema.

Los consumidores nos encontramos bastante indefensos ante las grandes empresas cuando se trata de proteger nuestra privacidad. Si bien es cierto que surgen leyes que amparan nuestra privacidad y fomentan un uso correcto de nuestros datos, en muchas ocasiones las empresas buscan resquicios legales para evadir estas leyes y lucrarse a costa de nuestra privacidad.

Este trabajo se estructura de la siguiente manera: en primer lugar, se contextualiza qué es la Revolución Digital y la sociedad digital en la que vivimos. Posteriormente, se analiza cómo esta era digital afecta a los consumidores y al marketing, para luego examinar las oportunidades y los riesgos que representa en distintos ámbitos. Finalmente, se aborda el tema del marketing y la privacidad del consumidor-ciudadano, complementado con seis ejemplos que exponen los graves problemas de privacidad que sufrimos como consumidores. En primer lugar, se analizan tres ejemplos relacionados con el marketing comercial y cómo las empresas se lucran de nuestros datos y de la gran cantidad de información que recopilan sin que los consumidores seamos plenamente conscientes. Los tres ejemplos restantes hacen referencia al marketing político y a lo valiosa que es para los partidos políticos la información personal de los consumidores, ya que estos son votantes en potencia.

La política hace mucho tiempo que se convirtió en algo científico, donde nada se deja al azar y todo está matemáticamente controlado. Los partidos no buscan agradar a todo el mundo; su único objetivo es lograr los votos suficientes para poder gobernar. Es por ello que tratan de apelar a nuestros sentimientos y emociones, como el miedo o la esperanza. Buscan que empaticemos con ellos para que luego seamos nosotros los que hagamos publicidad en su nombre. Para poder persuadirnos, primero deben conocernos, y para ello

utilizan toda la información que dejamos en internet. Crean perfiles de votantes y diseñan maneras de llegar a nosotros, ya que en esta época en la que vivimos, la política es una disciplina científica, milimetrada, y donde poco papel juega el azar.

Las similitudes entre el marketing comercial y el marketing político son evidentes. Ambos buscan influir en el comportamiento de un público objetivo y obtener un beneficio, ya sea en términos de votos (marketing político) o ventas (marketing comercial). Ciudadanos y consumidores son, en este contexto, dos caras de la misma moneda. En ambos casos, se intenta influir en nuestras decisiones, muchas veces manipulándonos para alcanzar estos fines. Desde ambas perspectivas, los ciudadanos-consumidores somos vistos como una oportunidad y una herramienta clave para lograr sus objetivos. Aunque también podemos encontrar algunas diferencias, como que el objetivo del marketing comercial está más orientado al largo plazo, mientras que el marketing político está centrado en lograr resultados a corto plazo.

Conocer el tipo de huella digital que dejamos y la repercusión que esta puede tener puede servirnos como medida preventiva para evitar posibles problemas futuros, como fraudes o compras impulsivas derivadas de publicidad personalizada, dirigida y específica hacia nosotros. Esto nos permitirá seguir tomando decisiones libres de influencias externas y tener una visión más clara y precisa del mundo real.

2. Objetivos

La Revolución Digital ha cambiado completamente la manera en que el consumidor se comporta y en que las empresas tratan a los consumidores, abriendo así la puerta a una gran cantidad de nuevas posibilidades.

Es por ello que los objetivos de este trabajo giran en torno a estos cambios, con el fin de detectar cuáles son sus puntos fuertes y débiles, y para poder defendernos como consumidores de estos últimos.

Los objetivos son:

- Analizar cómo han afectado al marketing y a los consumidores las nuevas tecnologías de esta era digital.
- Detectar las oportunidades y los riesgos que la Revolución Digital ha traído consigo.
- Examinar la situación de la privacidad del consumidor en el marketing comercial y la del ciudadano en el marketing político.

3. Metodología

En lo referente a la metodología utilizada en este trabajo, se emplearán principalmente dos métodos de investigación. Por un lado, se llevará a cabo una revisión bibliográfica de fuentes académicas, como libros, artículos publicados en revistas científicas y manuales especializados. Por otro lado, se consultarán fuentes no académicas, como noticias, páginas web y artículos de prensa.

En la primera parte del trabajo, que se enfoca en los aspectos teóricos de la Revolución Digital y la sociedad digital, así como su impacto en el marketing y los consumidores, se utilizarán como referencia libros académicos de autores como Jenkins (2006) y Brynjolfsson y McAfee (2014). Además, se incluirán artículos científicos de autores como Castells (2010), Chevalier y Mayzlin (2006), junto con estudios recientes como Saleslion (2024) y HubSpot (2020).

Para las dos próximas y últimas partes del trabajo, he tomado como base libros académicos como Römer (2014) y Kotler y Keller, (2020) y se ha seleccionado cada caso en base a una noticia.

En la segunda parte del trabajo, que aborda el tema del marketing comercial, se analizarán tres casos concretos. El primero, titulado "Pedir permiso para espiar", utilizará como base la noticia de *El País* “Deja que esta aplicación le rastree” Pascual (2021), complementada con información de Koetsier (2021). El segundo caso, titulado "Comodidad en casa pagada con tu privacidad", examinará productos de Amazon y las implicaciones para la privacidad de los consumidores, utilizando noticias de medios como Xataka y 20minutos. Finalmente, el tercer caso, "Demanda a Apple", se sustentará en la noticia “Apple es demandada por vender datos de sus usuarios a terceros” Hernández Ruza (2019).

La tercera y última parte del trabajo se centra en el marketing político y sigue una estructura similar a la del apartado anterior, dividiéndose en tres secciones. La primera, "Política personalizada", se refiere a la noticia de *El País* “Los partidos quieren tus datos” Galdon Clavell (2019). La segunda, "Facebook decide a quién debes votar", tratará sobre el escándalo relacionado con las elecciones de Estados Unidos de 2016. Finalmente, la tercera sección, "Tus datos a cambio de un billete de lotería", se centrará en la figura de Alvise Pérez y su promesa a la ciudadanía. Todo ello muy influenciado por la tesis de Sanchís (2014).

4. La Revolución Digital Y la Sociedad Digital

La Revolución Digital, también denominada la Tercera Revolución Industrial, es conocida como el proceso de transformación socioeconómico y tecnológico que comenzó en la segunda mitad del siglo XX, con la adopción e incremento de tecnologías digitales. Se define como la transición desde tecnologías analógicas y mecánicas a tecnologías digitales y electrónicas. Esta revolución ha implicado cambios fundamentales en diversos aspectos de la vida cotidiana, desde la manera en que nos comunicamos hasta la manera en que trabajamos y consumimos productos y servicios.

Según Castells (2010), la Revolución Digital puede entenderse como parte de una era más amplia de la información, caracterizada por la predominancia de las redes digitales y la informática. Castells (2010) argumenta que esta era de la información está marcada por la capacidad de las tecnologías de la información para procesar y distribuir inmensas cantidades de datos a alta velocidad, lo que ha transformado las estructuras económicas y sociales a nivel global. La informatización y la digitalización han llevado a la creación de nuevas formas de comunicación, tales como internet y las redes sociales, que han alterado profundamente la forma en que las personas interactúan, comparten información y participan en la vida pública.

La Revolución Digital se puede rastrear hasta el desarrollo de los primeros ordenadores y la invención del microprocesador en la década de 1970. Este período sentó las bases para la posterior evolución de la tecnología digital. La introducción del ordenador personal en los años 80 y la explosión de internet en los 90 fueron los principales detonantes que aceleraron la digitalización de la sociedad. Estos avances no solo hicieron que los ordenadores fueran más accesibles al público en general, sino que también allanaron el camino para la interconexión que ahora experimentamos a escala mundial. A medida que nos adentrábamos en el siglo XXI, la llegada de los dispositivos móviles y las redes sociales continuó esta tendencia de rápida transformación. Según el sociólogo Manuel Castells, estos avances no sólo han redefinido nuestra vida cotidiana, sino que también han reconfigurado las estructuras sociales y económicas de nuestra sociedad (Castells, 2010).

Uno de los cambios más significativos de la Revolución Digital es su impacto en la economía mundial. La digitalización ha facilitado el surgimiento de nuevos modelos de negocio, como las plataformas de comercio electrónico y la economía *gig*. La *gig economy*, o economía de trabajos esporádicos, se refiere a "un mercado laboral caracterizado por la prevalencia de contratos a corto plazo o trabajos *freelance* en lugar de empleos

permanentes" (Gillis, 2022). Este cambio ha sido impulsado por las plataformas digitales que conectan a los proveedores de servicios con los clientes de una manera fluida y eficiente.

En lo que a la economía se refiere, ha facilitado el surgimiento de la economía digital y el comercio electrónico, transformando modelos de negocio tradicionales y permitiendo la globalización de mercados. Empresas como Amazon, Google y Facebook han prosperado gracias a su capacidad para utilizar datos y tecnologías digitales de manera efectiva. La digitalización ha permitido, además, la automatización de procesos industriales, mejorando la eficiencia y reduciendo costos en la manufacturación y otros sectores productivos.

La integración de la automatización y la inteligencia artificial ha transformado significativamente el panorama laboral, provocando el desplazamiento de empleos tradicionales y abriendo, al mismo tiempo, nuevas oportunidades en sectores que han sido impulsados por la tecnología. Este cambio ha sido tan transformador que los economistas Brynjolfsson y McAfee lo han denominado la "segunda era de las máquinas" (Brynjolfsson y McAfee, 2014). En esta era, las competencias digitales han pasado a ser prioritarias para poder lograr ser competitivos en el mercado laboral.

Sin embargo, esta transición no ha estado exenta de desafíos. Han surgido problemas de desigualdad a medida que ciertos empleos se vuelven obsoletos, y existe una creciente preocupación por la capacidad de la mano de obra para adaptarse a estos cambios. La necesidad de aprendizaje continuo, de mejora y de reciclaje de las cualificaciones se ha vuelto más crítica que nunca para seguir el ritmo de este rápido avance tecnológico. Esta segunda era de las máquinas presenta tanto oportunidades como retos que deben abordarse si se pretende garantizar un crecimiento económico inclusivo y equitativo.

La Revolución Digital ha transformado significativamente la forma en que las personas se comunican y acceden a la información. Jenkins (2006) argumenta que las plataformas de redes sociales y otros canales digitales han permitido una mayor diversidad en la producción y distribución de contenidos, proporcionando oportunidades para que más personas puedan expresar sus ideas y ser escuchadas. Sin embargo, este nuevo panorama también ha planteado inquietudes en relación con la privacidad, la exactitud de la información y su impacto en la cohesión social.

La cultura de la inmediatez y la interconexión, fomentada por estas herramientas digitales, ha transformado significativamente las normas sociales y culturales. Actualmente, la gente espera recibir información al instante, y esta conectividad constante ha cambiado la forma

en que interactuamos entre nosotros y con el mundo que nos rodea. Aunque estas herramientas digitales han facilitado el intercambio y el acceso a la información, también han planteado nuevos retos que la sociedad aún está aprendiendo a afrontar. Mientras seguimos avanzando y adaptándonos a esta era digital, resulta de vital importancia equilibrar sus beneficios con la necesidad de proteger la privacidad individual, garantizar la veracidad de la información y mantener la armonía social.

A pesar de los innumerables beneficios, la Revolución Digital también presenta desafíos significativos. La ciberseguridad, la privacidad de los datos y la regulación de la inteligencia artificial son temas críticos que necesitan ser abordados. Además, la brecha digital sigue suponiendo un problema, con grandes diferencias en el acceso a tecnologías entre diferentes regiones y grupos en diferentes situaciones socioeconómicas.

En el futuro, la continua evolución de tecnologías emergentes como el Internet de las Cosas (IoT), la *blockchain* y la computación cuántica promete seguir transformando la sociedad de maneras impredecibles. La clave estará en equilibrar la innovación tecnológica con políticas inclusivas y sostenibles para asegurar que los beneficios de la digitalización sean ampliamente compartidos y, de esta manera, también poder garantizar una correcta privacidad del individuo y veracidad informativa. La Revolución Digital, además de transformar las interacciones sociales, ha revolucionado el marketing para empresas y consumidores, permitiendo un alcance sin precedentes, pero también imponiendo la responsabilidad de manejar los datos de manera ética y transparente.

5. La Revolución Digital: marketing y consumidores

La Revolución Digital ha transformado no solo las industrias y los mercados, sino que también las experiencias y comportamientos de los consumidores. Este profundo cambio ha sido impulsado por la masiva aceptación de tecnologías digitales, que han reescrito la manera en la que los consumidores interactúan con productos, servicios y marcas. A continuación, se procederá a analizar los efectos de la digitalización en el comportamiento del consumidor, examinando cómo las tecnologías digitales han cambiado la manera en que se busca información, se realizan compras y la forma en la que se interactúa con las empresas.

Un estudio realizado por GE Capital Retail Bank encontró que el 81% de los consumidores busca información sobre sus intereses de compra a través de internet antes de realizar compras importantes, destacando que esta búsqueda de información se realiza tanto cuando la compra se realiza en un entorno físico como cuando se lleva a cabo una compra en línea (Saleslion, 2024).

En la era digital en la que nos encontramos actualmente, los consumidores recurren cada vez más a internet como portal de búsqueda de información para ayudarles en la toma de decisiones, para comparar productos y leer opiniones antes de tomar una decisión de compra. Este comportamiento del consumidor nos permite ver la importancia que tienen la presencia en línea y las estrategias de marketing digital para las empresas, ya que cada vez más consumidores confían en estos recursos para orientar sus decisiones de compra (Saleslion, 2024). Además, según un estudio de Google e Ipsos, aproximadamente 8 de cada 10 consumidores siempre investigan en línea antes de realizar una compra para asegurarse de que están tomando la mejor decisión posible (Padilla, 2023). Además, otro informe destaca que los consumidores buscan valor, calidad y buen servicio al cliente, con el 53% optando por productos duraderos sobre los asequibles (Google, 2023).

Estos datos dejan clara la existencia de una tendencia creciente entre los consumidores de utilizar múltiples y diversos canales y dispositivos como herramientas para reunir información sobre productos y servicios antes de decidirse a comprarlos o adquirirlos. Entre las prácticas más habituales se incluyen comparar precios, leer reseñas de otros usuarios y buscar características específicas de los productos. Este tipo de comportamiento no se observa únicamente cuando se pretende adquirir productos de alto valor, sino que también

es común en compras de un carácter más habitual o incluso compras cotidianas y de menor valor.

El hecho de que se haya popularizado y normalizado escribir y dejar reseñas y opiniones en internet junto con la aparición de portales dedicados a ofrecer este tipo de servicio ha tenido un papel realmente importante y crucial en la toma de decisiones del consumidor. Plataformas como Yelp, TripAdvisor y Amazon permiten a los consumidores compartir sus experiencias y evaluar productos y servicios, lo que influye significativamente en las decisiones de compra de otros usuarios (Chevalier y Mayzlin, 2006). Por otro lado, muchos buscadores web, como puede ser el caso de Google, a la hora de buscar un lugar, como un restaurante o una tienda muestran directamente la media de las valoraciones otorgadas por los usuarios, que se mide en un rango que habitualmente oscila entre 0 y 5, donde 5 es la máxima puntuación. Esta puntuación aparece junto al nombre del local o comercio, es por ello que las empresas deben tener sumo cuidado con su imagen y la impresión que proyectan de cara al público, ya que este mismo público es el que procederá a otorgarle esta puntuación. Según un estudio de HubSpot (2024), el 77% de los consumidores confía tanto en las reseñas en línea como en las recomendaciones personales.

Figura 1: Reseña de Google

Fuente: Google

Los avances en tecnología de pagos, como las billeteras digitales o *wallets* y las criptomonedas y la tecnología que hay detrás de ellas, han facilitado aún más las transacciones en línea, aumentando la confianza del consumidor en el comercio electrónico (PwC, 2021). Los últimos avances en tecnología digital han permitido a las empresas ofrecer experiencias con un nivel de personalización altamente elevado a los clientes. A través del análisis de datos y la inteligencia artificial, las empresas pueden rastrear el comportamiento del consumidor y adaptar sus ofertas y comunicaciones a las preferencias individuales. Un informe de Accenture (2018) revela que el 91% de los consumidores es más probable que compren con marcas que les reconocen y que les proporcionan ofertas y recomendaciones relevantes basadas en sus gustos, intereses o compras anteriores.

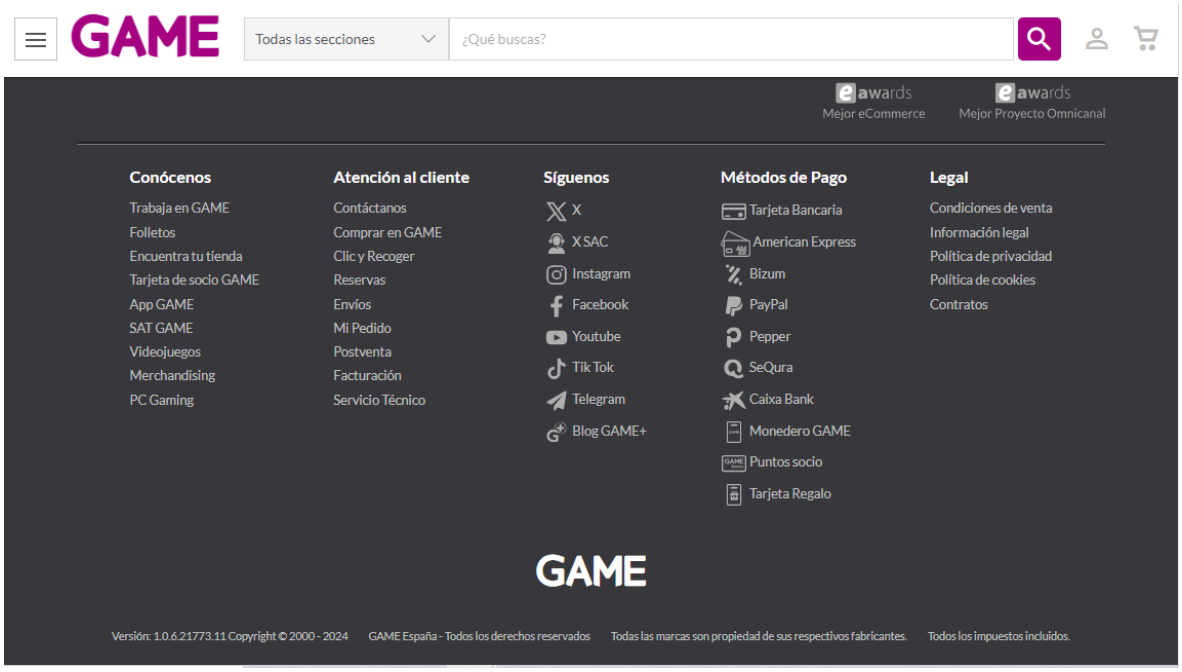
La personalización no solo mejora la satisfacción del cliente, sino que también aumenta la lealtad del cliente hacia la marca y el valor de vida del cliente (CLV, por sus siglas en inglés, *customer lifetime value*), que es una manera de medir los ingresos totales que la empresa espera obtener del cliente durante el tiempo que se prolongue la relación comercial entre ambas partes, lo cual permite a las empresas tomar decisiones más informadas acerca de qué cantidades de capital invertir en la adquisición de nuevos clientes o, como es el caso, en la retención de los ya existentes (Kumar y Shah, 2009).

Herramientas como *chatbots* y asistentes virtuales, impulsados por inteligencia artificial, también han mejorado el servicio al cliente, proporcionando respuestas rápidas y eficientes a las consultas de los consumidores (Panetta, 2018,). A pesar de considerarse un avance en muchos sentidos estos métodos en ocasiones causan un efecto negativo en los consumidores cuando estos no pueden resolver sus problemas o responder dudas, los cuales los consumidores sienten que un asistente humano podría solucionar.

La Revolución Digital ha transformado radicalmente las estrategias de comunicación y de marketing de las empresas. Las redes sociales, el marketing de contenidos y la publicidad digital permiten a las empresas llegar a audiencias de todo el mundo de manera más efectiva y económica que los medios tradicionales. Además, la capacidad de segmentación avanzada y la publicidad programática han permitido a los responsables de marketing dirigir sus campañas de manera más precisa, alcanzando al consumidor correcto en el momento adecuado (IAB, 2019). Hoy en día, es extraño que una empresa o marca no tenga presencia en diversas redes sociales, sobre todo en las más populares como Instagram, Facebook, X o TikTok. Estas plataformas presentan una enorme ventana de exposición al

mundo y una manera más sencilla y barata de llegar a un público más amplio que mediante métodos tradicionales; además, muchas compañías facilitan el acceso a sus perfiles en redes sociales desde su propia página web.

Figura 2: Enlace a redes sociales



Fuente: GAME España (2024).

La segmentación avanzada consiste en utilizar datos precisos y detallados sobre los consumidores y sus hábitos para así poder dividir el mercado y crear campañas de marketing más efectivas y dirigidas de manera personalizada (Wedel y Kamakura, 2000).

Por otro lado, la publicidad programática se refiere a al uso de software y algoritmos automatizados para la compraventa de espacios publicitarios en tiempo real, lo que permite que estos se dirijan automáticamente a una audiencia específica lo que optimiza la efectividad y la eficiencia de las campañas publicitarias (Goldfarb y Tucker, 2011).

El proceso de digitalización, si bien aporta numerosos beneficios, también presenta grandes desafíos. Entre los desafíos más importantes se encuentran las cuestiones relacionadas

con la privacidad de los datos y la seguridad de la información. Según Norton LifeLock. (2021), Informe Norton sobre Seguridad de Datos 2021, un considerable 44% de los consumidores expresa su preocupación por la privacidad de sus datos en línea. Según un informe de Deloitte (2023), un 67% de los usuarios de teléfonos inteligentes y dispositivos para el hogar inteligente están preocupados por la seguridad y privacidad de sus datos en dichos dispositivos, lo que representa un incremento respecto a años anteriores. Esta preocupación está más que justificada debido a la creciente dependencia que se ha creado de las plataformas digitales para la realización de diversas actividades, las cuales a menudo implican compartir información sensible.

Además, la influencia de los algoritmos y la posible manipulación de la información nos obligan a plantearnos varias cuestiones éticas sobre el poder que ostentan las plataformas digitales. Estas plataformas cuentan con la capacidad de moldear las decisiones de los consumidores y la opinión pública, lo que puede tener implicaciones de gran alcance (Zuboff, 2019).

5.1 Oportunidades y riesgos

5.1.1. Oportunidades

Acceso a Productos y Servicios:

La Revolución Digital ha facilitado significativamente el acceso a productos y servicios, eliminando las barreras geográficas que hasta ahora restringían las opciones de compra de los consumidores. Los consumidores ahora pueden comprar desde cualquier lugar del mundo, acceder a una enorme variedad de productos y comparar precios y características con facilidad nunca antes vista. Plataformas como Amazon, Alibaba y eBay han permitido que los usuarios puedan acceder a productos de cualquier parte del mundo con tan solo unos clics (Brynjolfsson, Hu, y Rahman, 2013). El comercio electrónico y las plataformas de venta online han facilitado la disponibilidad de productos especializados y de nicho que antes eran difíciles de encontrar, además de ofrecer una mayor variedad de precios entre los que barajar opciones de compra (Cavallo, 2017). Esto se traduce en la posibilidad de tomar decisiones más informadas, gracias a poder comparar características, y más económicas, gracias a la comparación de precios (Flavián, Gurrea, y Orús, 2016).

Al mismo tiempo, una de las mayores mejoras que ha traído consigo la digitalización del mercado ha sido la comodidad en el proceso de compra. Esto se debe a que no únicamente se ha eliminado la barrera geográfica, sino que también se ha eliminado una barrera temporal que impedía a los consumidores acceder al proceso de compra. Gracias al avance en los dispositivos móviles y las aplicaciones de comercio electrónico se ha eliminado la necesidad de desplazarse físicamente a un punto de venta, lo cual se traduce en un ahorro de tiempo y esfuerzo, es decir, el consumidor ha ganado comodidad (Pantano y Viassone, 2015).

Personalización:

Las tecnologías digitales permiten a las empresas recolectar y analizar datos del comportamiento del consumidor, lo que les facilita ofrecer productos y servicios personalizados basándose en dichos datos. Esta personalización puede mejorar la experiencia del cliente, hacer recomendaciones más relevantes y, como resultado, un aumento de la satisfacción del consumidor. Esto se logra gracias al uso de grandes volúmenes de datos y algoritmos de aprendizaje automático; lo que popularmente se conoce como inteligencia artificial (IA). Estas tecnologías son entrenadas para realizar análisis del comportamiento y preferencias de los consumidores para, de esta manera,

poder ofrecer recomendaciones personalizadas basadas en los intereses o necesidades de cada consumidor (Adomavicius y Tuzhilin, 2005). Gracias a la personalización se logra mejorar la experiencia del cliente además de aumentar la probabilidad de satisfacción y la lealtad del mismo (Tong, Wong y Lui, 2017).

Facilidad de Comunicación:

La comunicación entre las personas, tanto la manera de hacerlo como los medios utilizados para ello, es uno de los factores que más se ha visto influido por la Revolución Digital. Las facilidades que nos ha otorgado la tecnología para relacionarnos ha facilitado la aparición de nuevos modelos de negocio que benefician a los consumidores. Un ejemplo de esto es la economía colaborativa, la cual permite a las personas compartir recursos y servicios a través de plataformas digitales. Empresas como Airbnb o Uber han logrado revolucionar sus respectivos sectores gracias a su propuesta de alternativas más accesibles y, en muchos casos, más económicas que su contraparte de servicios tradicionales, que en el caso de estas dos empresas se trataría de los servicios de hoteles y taxis, entre otros (Sundararajan, 2016). Estos nuevos modelos de negocio no solo ofrecen mayor flexibilidad para los usuarios, sino que también crean nuevas oportunidades económicas que pueden aprovechar.

La evolución de las plataformas digitales como redes sociales y foros en línea ha mejorado significativamente el ámbito de la comunicación entre consumidores y empresas. Estos espacios digitales ofrecen a los consumidores la oportunidad de expresar sus opiniones, participar en interacciones de atención al cliente y formar parte de comunidades en línea. En estos espacios digitales se pueden compartir experiencias personales, intercambiar recomendaciones y participar en debates, lo cual fomenta así un sentimiento de compañerismo y solidaridad.

Al realizar una escucha activa y atender de manera responsable las necesidades de su clientela en estos foros, las empresas pueden lograr construir relaciones duraderas y significativas con sus clientes, facilitando así un futuro camino hacia un diálogo abierto, transparente y que resulte beneficioso tanto para la empresa como para el cliente. Las plataformas digitales han transformado la interacción entre consumidores y empresas, permitiendo a las marcas escuchar activamente y responder a las necesidades de sus clientes. Esta interacción bidireccional no solo mejora la experiencia del cliente, sino que también fortalece las relaciones a largo plazo (Leeflang, Verhoef, Dahlström y Freundt, 2014).

El impacto de las redes sociales en la relación empresa-cliente es claro, ya que la posibilidad de recibir retroalimentación directa y participar en discusiones mejora el compromiso del consumidor con la marca, fortaleciendo la lealtad a largo plazo (Kaplan y Haenlein, 2010). Asimismo, la transformación digital permite a las empresas interactuar de manera más eficiente y cercana, adaptándose a las nuevas demandas de los consumidores.

Educación y Entretenimiento:

El acceso a la información y a la educación es otra área donde la Revolución Digital ha creado importantes oportunidades para el consumidor, ya que les ha proporcionado acceso a una amplia variedad de recursos educativos y de entretenimiento. Plataformas de *e-learning*, bibliotecas digitales y servicios de *streaming* ofrecen contenido educativo y de entretenimiento, como Coursera, edX y Khan Academy, las cuales permiten a los consumidores acceder a una educación de alta calidad desde cualquier lugar del mundo, muchas veces de forma gratuita o a bajo costo (Yuan y Powell, 2013). Esta apertura al conocimiento facilita un acceso más igualitario a la educación y brinda a las personas la oportunidad de adquirir nuevas habilidades y mejorar sus perspectivas laborales. También permite que los profesionales se mantengan actualizados en sus áreas de trabajo y accedan a oportunidades de desarrollo continuo (Pappano, 2012)."

5.1.2. Riesgos

A pesar de los innumerables beneficios que ha traído consigo la Revolución Digital para los consumidores, este nuevo entorno digital también conlleva una serie de riesgos relacionados con la privacidad, la seguridad y el bienestar de los consumidores. A continuación se va a proceder a examinar los principales riesgos asociados con la Revolución Digital desde el punto de vista de los consumidores, haciendo hincapié en la importancia que tiene el conocimiento, la anticipación y la prevención de los problemas para poder abordarlos de una manera en la que se pueda proteger al consumidor de los mismos.

Privacidad y Seguridad

Uno de los riesgos más destacados de la Revolución Digital es la pérdida de la privacidad. La recopilación masiva de datos personales por parte de empresas y plataformas digitales plantea serias preocupaciones sobre la privacidad y la seguridad. A medida que los usuarios interactúan con plataformas en línea generan, muchas veces de manera inconsciente, una gran cantidad de datos personales que pueden ser recopilados, almacenados, procesados y utilizados por las empresas. Los consumidores corren el riesgo de que sus datos sean utilizados sin su consentimiento o expuestos a violaciones de seguridad o ciberataques que tengan como objetivo la recolección de datos. Los datos más comúnmente proporcionados por los consumidores, que además podemos considerar como información sensible, son nombres y apellidos, fechas de nacimiento, direcciones, números de teléfono, direcciones de correo electrónico y patrones de comportamiento, los cuales pueden ser utilizados para crear perfiles detallados de dichos consumidores (Solove, 2006). La recolección masiva de estos datos ha dado pie a que los usuarios comiencen a preocuparse acerca de la forma en la que las empresas manejan y almacenan estos datos. El uso indebido de estos datos para manipular las decisiones de compra de los consumidores o la venta de estos datos también da lugar a preocupaciones debido al potencial que tienen para poder abusar del consumidor (Acquisti, Brandimarte, y Loewenstein, 2015).

Por otro lado, el riesgo y la exposición a ciberataques es un factor que afecta enormemente a los consumidores en esta era digital en la que vivimos. A cada día que pasa, más aspectos de la vida cotidiana se digitalizan, lo que incrementa tanto el interés como la facilidad de las amenazas cibernéticas, tales como robos de identidad, fraudes o violaciones de datos. Es común que los ciberdelincuentes traten de explotar las debilidades en la

seguridad de las páginas web y portales en línea con el fin de obtener acceso no autorizado a la información personal de los consumidores, entre otras actividades ilícitas.

Protegerse estos ataques cibernéticos no es barato para las empresas, pero es un pequeño precio a pagar con tal de tratar de mantener los datos privados de sus usuarios a salvo, ya que una filtración de estos datos suele tener como resultado, la mayoría de las veces, una pérdida a nivel financiero para la empresa. Además, hay que sumar el daño a su reputación y la pérdida de confianza por parte de los clientes (Anderson y Moore, 2007). Según una investigación de Symantec (2018), los ataques de *phishing* y *malware* han aumentado considerablemente, lo que hace resaltar la necesidad de mejorar las prácticas de seguridad por parte de las empresas y no dejar de lado la necesidad de educar a los consumidores sobre los riesgos cibernéticos. Según Malwarebytes (s. f.), "el *phishing* es un tipo de ciberdelito en el que se engaña a los usuarios para que revelen su información personal identificable" (párr. 1).

Sobrecarga de Información

La enorme cantidad de información que se encuentra disponible en línea puede llevar a una sobrecarga de información, la cual hace que los consumidores se sientan abrumados por la cantidad de datos y opciones que encuentran a su disposición. La constante exposición a grandes cantidades de información a través de múltiples canales hace que sea más habitual que el consumidor se encuentre con dificultades a la hora de evaluar y procesar información de manera efectiva y así ser capaz de diferenciar entre la información que es relevante para la toma de decisiones y la que no (Eppler y Mengis, 2004). Esto se traduce en una mayor dificultad para lo que se conoce como toma de decisiones informada, y, además, aumenta la ansiedad en los consumidores, quienes se sienten abrumados por la cantidad de opciones que encuentran a su disposición; a este fenómeno se le conoce como fatiga digital.

Desinformación y Manipulación

El tener acceso a tanta información obliga a los consumidores a aprender a filtrar la información relevante, saber detectar información no relevante y, además, identificar qué información es falsa o está manipulada. El aumento de la desinformación y de la manipulación de la información en línea es otro de los riesgos más destacables de la era digital. En los últimos años, sobre todo debido a las redes sociales, se ha facilitado que la información se difunda de manera rápida y a gran escala tanto de la información verídica como de la no verídica o la no contrastada. Gracias a las redes sociales y al hecho de que los usuarios tienden a compartir información entre ellos, se vuelve más sencillo hacer pasar

una información por verdadera cuando en realidad no lo es. Según Wardle y Derakhshan (2017), la propagación de noticias falsas y la desinformación a través de las redes sociales ha aumentado de manera exponencial, impulsada por la falta de filtros y la velocidad con la que se comparte contenido en estas plataformas.

Los usuarios tienden a compartir con sus “seguidores” información que va acorde a sus ideales, sin muchas veces contrastar la veracidad de dicha información. Este fenómeno es conocido como “ecosistema de desinformación” en el cual las personas refuerzan sus creencias mediante una exposición repetida a información falsa o sesgada (Lazer et al., 2018). Este hecho provoca que se forme una cadena de personas que ha compartido una información que podría resultar no ser verdadera o estar incompleta y que están mal informando a otros usuarios. Aunque estos últimos no compartan la información, es probable que interioricen la información y puede que no lleguen a cuestionarse su veracidad.

La desinformación es tan peligrosa como la mala información, y el hecho de haber recibido información errónea puede llegar a influir en las percepciones y decisiones de los consumidores. El hecho de tomar una decisión basada en información errónea puede llevar a una pérdida de confianza en las plataformas digitales lo que afecta negativamente tanto a las empresas como a los usuarios (Allcott y Gentzkow, 2017). Según un estudio de Lewandowsky, Ecker y Cook (2017), una vez que una creencia errónea ha sido formada con una base de información errónea o falsa, es muy difícil corregirla, lo que recalca la gravedad de la desinformación en la toma de decisiones de los consumidores.

Tras varios años de análisis y aprendizaje acerca de las posibilidades que ofrece la era digital, las empresas han logrado desarrollar técnicas de marketing digital avanzadas, como la publicidad dirigida. Estas técnicas pueden llegar a manipular el comportamiento de los consumidores gracias a la explotación de las preferencias y las vulnerabilidades de los mismos. Esto plantea unas serias preocupaciones éticas acerca del poder que tienen las compañías para influir en las decisiones de los consumidores (Zuboff, 2019). De hecho, estudios recientes han señalado que este tipo de prácticas puede llegar a generar una pérdida de autonomía en los consumidores, al ser influenciados de manera sutil y continua en sus decisiones de compra (Susser, Roessler y Nissenbaum, 2019).

Fraude y Estafas en Línea

El incremento del comercio electrónico también ha llevado a un aumento en el número de fraudes y de estafas en línea. Los consumidores pueden ser víctimas de transacciones

fraudulentas, sitios web falsos o copias de sitios originales, entre otras muchas formas de engaño digital. La Revolución Digital ha dado lugar a un aumento significativo de fraudes y estafas, ya que ha abierto un nuevo canal en el que los delincuentes pueden operar, lo cual representa un grave riesgo para los usuarios de las tecnologías digitales. Según un informe de la Comisión Federal de Comercio (FTC) en 2020, las denuncias por fraudes en línea superaron los $3.3 mil millones en pérdidas, lo que refleja un preocupante aumento en comparación con años anteriores (FTC, 2020).

Las estafas y los fraudes en línea afectan a millones de consumidores a nivel global. Estos consumidores suelen sufrir consecuencias a nivel financiero y en muchas ocasiones también pueden llegar a afectar psicológicamente al consumidor, generando estrés, ansiedad y desconfianza hacia el comercio digital (Button, Nicholls, Kerr y Owen, 2014). Aunque la cantidad de fraudes diferentes que existen hoy en día es imposible de contar, sí es posible clasificarlos según la manera en la que actúan o en lo que se centran en conseguir.

El *phishing* es una de las formas más comunes de fraude en línea, y no por ello representa una amenaza menor para el consumidor. Como hemos mencionado anteriormente, el objetivo del *phishing* es la obtención de información sensible de los usuarios. El *phishing* es un tipo de estafa es muy común en portales de venta C2C, sobre todo en portales de venta de segunda mano. La práctica más habitual es mediante el envío de correos electrónicos, mensajes de texto o enlaces fraudulentos que imitan la apariencia de comunicaciones verídicas con el fin de engañar al consumidor. El objetivo principal, como bien se ha mencionado, es que el consumidor revele información personal sensible como contraseñas, números de tarjetas de crédito, direcciones, identificaciones o datos bancarios.

Según un informe de la empresa de seguridad cibernética Symantec (2018), los ataques de *phishing* han aumentado considerablemente en los últimos años, convirtiéndose en una de las principales amenazas en línea. Además, un estudio de Verizon (2021) revela que el 36% de todas las filtraciones y robo de datos fueron causados por ataques de *phishing*, lo que nos permite hacernos una idea del tipo amenaza digital ante la que nos encontramos. El robo de identidad resultante tras sufrir uno de estos ataques no solo genera pérdidas económicas, sino que también puede dañar la reputación de las víctimas y afectar su bienestar emocional (Anderson y Moore, 2007). Los consumidores suelen enfrentarse a la dificultad añadida de querer recuperar su dinero o de tomar acciones legales contra los estafadores, quienes a menudo operan desde jurisdicciones extranjeras.

A medida que las compras en línea se vuelven más habituales y más consumidores recurren a ellas, más aumenta la probabilidad de que los consumidores se encuentren con páginas web fraudulentas que se hagan pasar por páginas legítimas o tiendas oficiales. La manera de actuar de estas falsas tiendas pasa desde poner a la venta productos inexistentes o falsificados, hasta no enviar los productos comprados por el consumidor. Un estudio realizado por Newman y Clarke (2013) muestra que estas estafas pueden ser altamente sofisticadas, al fin y al cabo en parecer real radica su clave del éxito, utilizando métodos avanzados de ingeniería social para convencer a los consumidores de la autenticidad del sitio web. Además, según un informe de Europol (2020), las estafas relacionadas con el comercio electrónico, incluidas las tiendas falsas, han crecido considerablemente, afectando a millones de consumidores en todo el mundo.

Si bien las formas de pago en línea han facilitado enormemente las transacciones comerciales, también han creado oportunidades para el fraude. La utilización de tarjetas de crédito o sistemas de pago digitales vuelve a los consumidores vulnerables a percibir cargos fraudulentos, duplicaciones de pagos, clonaciones de tarjetas bancarias o el desvío de fondos a otras cuentas. Según un informe de la Comisión Federal de Comercio de Estados Unidos (2020), las quejas relacionadas con fraudes en pagos digitales han aumentado considerablemente, por lo que destaca la necesidad de medidas de seguridad más estrictas y severas. Además, un estudio de Javelin Strategy & Research (2021) reveló que las pérdidas por fraudes en pagos digitales alcanzaron cifras récord, subrayando la urgencia de una mayor concienciación por parte de los consumidores y la implementación de medidas preventivas (Buzzard y Kitten, 2021)

La actividad financiera de los usuarios no se limita únicamente a realizar pagos en línea; con la llegada de los teléfonos inteligentes y el fácil acceso a ellos, ya que su precio no suele suponer una barrera a la horade adquirirlos, ahora también gestionan su dinero de manera telemática gracias a internet mediante servicios financieros en línea y aplicaciones móviles. En el ecosistema digital en el que nos encontramos, es común encontrarse con estafas relacionadas con préstamos fraudulentos, esquemas de inversión falsos y otras formas de fraude financiero. Estas estafas se aprovechan de las necesidades financieras de los consumidores y de su desesperación por obtener crédito de manera rápida y sencilla, lo que a menudo acaba como resultado con la pérdida de ahorros y una acumulación de deudas (Lustig y Nardi, 2015). Las plataformas de finanzas digitales, aunque en muchas ocasiones pueden ser convenientes y beneficiosas para el consumidor, resultan ser un arma de doble filo si estas no se encuentran debidamente reguladas o si los consumidores no han

recibido una adecuada educación sobre las posibles amenazas y riesgos que este tipo de portales en línea pueden tener.

Para poder prevenir, y en caso de que ya haya sucedido, mitigar todos estos riesgos y el daño que puedan, causar es necesario un esfuerzo tanto por parte de las autoridades como de las empresas tecnológicas. Los consumidores necesitan una mayor y mejor concienciación y educación acerca de los riesgos que pueden encontrarse y de las maneras que existen para protegerse de ellos en esta era digital.

Brecha Digital y Exclusión

La era digital ha cambiado la vida de las personas en todos los aspectos de la misma. La tecnología está presente en prácticamente todos los aspectos de la vida cotidiana. Cuando hablamos de la brecha digital, nos referimos a la desigualdad en el acceso y uso de las tecnologías de la información y la comunicación (TIC), lo que puede limitar las oportunidades para quienes no tienen acceso adecuado. Según van Dijk (2006), "la brecha digital se define como la distancia entre aquellos individuos que tienen acceso pleno a las tecnologías digitales y aquellos que no pueden utilizarlas por falta de acceso, habilidades o motivación" (p. 222).

El cambio drástico que ha sufrido la vida cotidiana debido a la inclusión de la tecnología en todos los ámbitos de la vida cotidiana ha hecho que haya que adaptarse a los cambios que trae consigo la era digital. La brecha digital es uno de los desafíos más importantes que ha traído consigo la Revolución Digital. A pesar de que la conectividad ha tenido una expansión global generalizada, aún existen desigualdades significativas en el acceso a estas tecnologías digitales. Estas desigualdades están basadas en factores geográficos, educativos o socioeconómicos, lo que causa que existan una serie de grupos que estén excluidos de los beneficios de la digitalización (van Dijk, 2006).

La ausencia de un acceso adecuado a internet y a dispositivos tecnológicos, así como la incapacidad o falta de adaptación a estas tecnologías, tiene como consecuencia limitar las oportunidades de los consumidores para poder participar de manera plena en la economía digital, aumentando de esta manera las diferencias que ya existían y dando lugar así a una nueva forma de exclusión social (Hilbert, 2011).

6. El marketing y la privacidad del consumidor

La privacidad del consumidor se ha convertido en uno de los temas que más preocupación genera en la era digital, la cual está marcada por el auge de tecnologías de la información y la comunicación. El auge del *Big Data*, las redes sociales y el marketing digital han transformado la forma en que las empresas recopilan, almacenan y utilizan los datos de los consumidores, generando así nuevas oportunidades, pero también importantes riesgos en lo que a la privacidad respecta. Esta situación plantea serios desafíos tanto para los consumidores como para las empresas y organizaciones, las cuales deben lograr un cierto nivel de equilibrio entre eficiencia y personalización de sus estrategias de marketing, a la vez que garantizar el respeto a la privacidad y la protección de los datos personales de los consumidores.

La creciente preocupación por la privacidad ha llevado a la implementación de regulaciones más estrictas, como el Reglamento General de Protección de Datos (GDPR) en Europa, diseñado para otorgar a los usuarios mayor control sobre su información personal (Tikkinen-Piri, Rohunen y Markkula, 2018). Sin embargo, muchas empresas todavía luchan por cumplir con estos requisitos sin comprometer su capacidad para utilizar los datos de manera efectiva.

Como consecuencia de la Revolución Digital, los datos que se deben procesar hoy en día no pueden ser gestionados por herramientas tradicionales de procesamiento de datos. A la capacidad de procesar y analizar estos grandes volúmenes de datos se le conoce como *Big Data*. En el ámbito del marketing digital, el *Big Data* permite a las empresas obtener *insights* profundos sobre los comportamientos, preferencias y necesidades de los consumidores (Tene y Polonetsky, 2013). Como señalan Tene y Polonetsky (2013), "los *insights* derivados del *Big Data* permiten a las organizaciones tomar decisiones más informadas y personalizadas, mejorando la eficiencia y relevancia de sus acciones" (p. 240). Sin embargo, esta capacidad de análisis de datos trae consigo una contraparte: las preocupaciones sobre la privacidad de dichos datos, ya que la recolección masiva de datos puede dar lugar a identificación y perfilado de consumidores sin su consentimiento (Acquisti, Brandimarte, y Loewenstein, 2015). El uso de *Big* Data en el marketing digital crea una paradoja: mientras más precisa y personalizada sea la estrategia de marketing, mayor es el riesgo de violación de la privacidad del consumidor.

Uno de los avances más significativos que ha traído consigo la era digital y que más ha alterado el estilo de vida de los usuarios es la aparición de las redes sociales. Si bien las

redes sociales han revolucionado la manera en la que las personas nos comunicamos y compartimos información, es en esta segunda parte donde también se halla el problema. A la vez que han aparecido nuevas maneras de comunicarse, se han abierto nuevos caminos para recopilar y explotar datos personales.

Plataformas digitales tales como Facebook, Twitter (actualmente X) o Instagram tienen una finalidad “oculta”; además de la obvia que es la de actuar como medios de comunicación. Estos portales digitales sirven como lugares donde recopilar enormes cantidades de información y de datos de sus usuarios, la cual posteriormente es utilizada para poder dirigirles publicidad y contenido personalizado a esos mismos usuarios (Andrejevic, 2011). Esta práctica ha sido el centro de muchas controversias y debates sobre la privacidad, ya que en muchas ocasiones los usuarios de estas plataformas no son consciente, al menos plenamente, del alcance de la recopilación de sus datos ni de qué manera van a ser procesados, tratados y utilizados, ya sea por las mismas plataformas o por terceros (Zuboff, 2019).

En las redes sociales, se comparte información personal con lo que podría calificarse como demasiada facilidad, lo cual puede llevar a una exposición involuntaria e innecesaria de privacidad. Esta exposición puede traer consigo graves consecuencias, tales como el robo o suplantación de identidad, o la manipulación de comportamientos del consumidor a través de algoritmos de recomendación y publicidad dirigida.

Los algoritmos de recomendación utilizan como base el análisis de grandes volúmenes de datos recopilados de los usuarios, como su historial de compras, hábitos de negociación, interacciones en redes sociales y sus preferencias declaradas (Adomavicius y Tuzhilin, 2005). Estos algoritmos utilizan técnicas avanzadas de *machine learning*, que es “una disciplina de la inteligencia artificial que permite a los ordenadores aprender por sí mismos y realizar tareas de forma autónoma sin necesidad de ser programados” (Iberdrola s. f.), para identificar patrones en los datos que se les proporciona y, en este caso concreto, predecir qué tipo de productos o servicios podrían ser de interés para el usuario.

Una vez obtenida esta información, se usa para poder realizar recomendaciones al consumidor. La publicidad dirigida trabaja de una manera bastante similar, ya que emplea estos datos para así poder mostrar anuncios personalizados que coincidan con los gustos o intereses específicos de cada consumidor, lo cual genera una mayor posibilidad de conversión (Sundararajan, 2017). Según Goldfarb y Tucker (2011), "la publicidad dirigida

utiliza información sobre el comportamiento del consumidor para presentar anuncios más relevantes, incrementando la efectividad de las campañas publicitarias" (p. 390).

Para lograr hacer un uso correcto y eficiente del funcionamiento de este tipo de prácticas o técnicas, es indispensable haber realizado y tener a disposición una extensa recopilación de datos personales. Podemos considerar como un grave riesgo la falta de transparencia en la manera de obtener estos datos y la manera de obtener un consentimiento informado por parte de los consumidores. En la gran mayoría de las ocasiones, los consumidores no son plenamente conscientes de la cantidad de datos que se van a recopilar, el tipo de datos y el posterior tratamiento y uso de los mismos para influir en su comportamiento (Acquisti, Brandimarte, y Loewenstein, 2015). La opacidad en las políticas de privacidad y la complejidad de los algoritmos dificultan que los consumidores comprendan el alcance del control que las empresas tienen sobre sus datos personales. Esta falta de transparencia puede llevar a una erosión de la confianza del consumidor y generar una percepción negativa hacia las empresas que utilizan estas tecnologías, influyendo así de manera negativa en su imagen de marca (Martin, Borah y Palmatier, 2017).

Al aprovechar los datos personales, las empresas pueden influir en las decisiones de compra y en las preferencias de los usuarios de maneras que estos no anticipan o entienden completamente (Eslami et al., 2015). Este tipo de manipulación mediante algoritmos puede limitar la autonomía y el libre albedrío del consumidor, ya que las recomendaciones y los anuncios personalizados pueden dirigir a los consumidores hacia opciones que benefician más a la empresa que al propio consumidor. Además, los algoritmos de recomendación y la publicidad dirigida pueden agravar problemas como la adicción al consumo y el sobreendeudamiento, ya que promueven de manera incesante productos y/o servicios que, aunque sean de interés para el consumidor, en muchas ocasiones no son necesarios, lo conlleva a que no sopesen otras opciones y puede llevar a compras impulsivas.

El marketing digital ha evolucionado hacia un enfoque altamente personalizado, donde es habitual que las empresas utilicen datos de comportamiento, demográficos, geográficos y socioeconómicos para crear campañas de marketing dirigidas con el fin de maximizar la relevancia y el impacto de las mismas. Como hemos comentado previamente, este suceso se da gracias al *Big Data*, el cual es posible gracias a la integración de tecnologías de vigilancia comercial, como son las cookies y los píxeles de seguimiento, que permiten a las empresas rastrear las actividades en línea de los consumidores en tiempo real (Turow, 2011).

Sin embargo, esta vigilancia intrusiva plantea serias cuestiones éticas y legales relacionadas con la privacidad. La recopilación y el análisis de datos sin el conocimiento explícito del usuario pueden llevar a una sensación de pérdida de control sobre la propia información personal, lo que a su vez puede erosionar la confianza en las marcas y en el entorno digital en general (Martin y Murphy, 2016).

Sin embargo, los datos recopilados de los consumidores no se utilizan únicamente con fines no éticos por parte de las empresas. Esta cantidad de datos pueden ser utilizados y aprovechados para comprender mejor a los consumidores y desarrollar productos y servicios que se ajusten a las necesidades y preferencias individuales de cada consumidor, o mejorar los ya existentes con el fin de lograr una satisfacción global mayor. Sin embargo, estas oportunidades vienen acompañadas de un desafío en cuanto a la gestión ética y legal de los datos personales de los consumidores. Las empresas se encuentran en un entorno regulatorio que se vuelve más complejo cada vez, donde se ven obligados a cumplir con leyes como el Reglamento General de Protección de Datos (GDPR) en Europa, que imponen estrictas obligaciones sobre la recopilación, el almacenamiento y el uso de los datos de los consumidores (Voigt y Von dem Bussche, 2017).

Actualmente, nos encontramos en un mercado donde el consumidor es cada vez más consciente y exigente en lo que a la protección de su información personal se refiere. Que una empresa opte por un enfoque transparente y respetuoso hacia la privacidad de sus usuarios puede llegar a convertirse en una importante ventaja competitiva. Es por ello que las empresas deben considerar el impacto que tendrá el uso que le den a los datos de sus usuarios y la repercusión de ello en la percepción de la marca por parte del público y la lealtad del consumidor (Martin, Borah y Palmatier, 2017).

La privacidad del consumidor en la era digital es un tema complejo que involucra múltiples factores, incluyendo a empresas, reguladores y a los propios consumidores. La capacidad de recopilar y analizar grandes cantidades de datos ofrece oportunidades únicas para la personalización y la eficiencia en el ámbito del marketing, pero también plantea importantes desafíos éticos y legales. A medida que la tecnología continúa evolucionando, será crucial que las organizaciones tomen medidas y desarrollen acciones que respeten la privacidad del consumidor, no solo con el fin de cumplir con las normativas legales y evitar posibles futuras sanciones, sino también para mantener la confianza y la lealtad de los usuarios en un entorno digital que se vuelve cada vez más competitivo.

A continuación vamos a proceder a analizar una serie de casos que remarcan la importancia y el valor que tienen nuestros datos para las empresas y los diversos usos que estos datos tienen.

6.1. El marketing comercial y la privacidad del consumidor:

6.1.1. Pedir permiso para espiar

Apple plantó cara a los términos de privacidad de los usuarios y al mercado publicitario digital con su actualización iOS 14.5, actualización que fue lanzada el 26 de abril de 2021. Gracias a esta actualización, los usuarios podían, por primera vez, decidir si las aplicaciones instaladas en sus dispositivos móviles pueden o no recopilar datos con fines publicitarios; las cuales hasta el momento lo hacían por defecto y sin previo aviso, y estos datos se compartían con empresas anunciantes y *brokers* de datos. Esta función, conocida como *App Tracking Transparency* (ATT), permite a los usuarios optar por no ser rastreados por las aplicaciones, lo que representa un gran cambio en la forma en que se gestionan los datos personales en el ecosistema digital (Apple, 2021).

Este cambio no repercute únicamente a Apple. Nueve grandes empresas alemanas de medios de comunicación, tecnología y publicidad acusaron a Apple de haber quebrantado las reglas antimonopolio, argumentando que los cambios realizados en su política de privacidad dañarían el mercado publicitario. Según el *Financial Times*, periódico britanico especialista en noticias internacionales de carácter económico, estas empresas sostienen que la introducción de la función *App Tracking Transparency* (ATT) limitará gravemente el acceso a datos cruciales para la publicidad dirigida, lo que afectará tanto a anunciantes como a brókeres de datos (*Financial Times*, 2021). Las empresas afirman que esto otorgaría a Apple una ventaja injusta sobre los competidores, ya que controlaría tanto el acceso a los datos como el ecosistema publicitario en sus dispositivos.

Entre las empresas afectadas se encuentra, la empresa fundada por Mark Zuckerberg. Junto con Google, esta empresa domina el mercado de procesamiento de datos de usuario con el fin de ofrecer publicidad, por lo que podemos afirmar que esta empresa vive de estos datos de sus usuarios. Aquellos usuarios de Apple que rechacen el seguimiento de su actividad en la aplicación de Facebook dejarán de recibir publicidad personalizada, lo cual supone una pérdida significativa para Facebook, ya que su modelo publicitario depende en su mayoría de poder ofrecer publicidad personalizada a sus usuarios (Business Insider, 2021).

Viendo el revuelo que estaba surgiendo alrededor de la decisión tomada por la compañía, Apple se mostró firme en su decisión y enfatizó la importancia de la privacidad de los usuarios, haciendo hincapié en que ellos mismos deben ser quienes decidan si sus datos

deben de ser analizados y procesados por terceros. La empresa también aprovechó para resaltar que sus nuevas reglas de privacidad se aplican de manera uniforme a todos los desarrolladores y que no tienen como objetivo la discriminación de ninguno de ellos. Aun así, se baraja un posible motivo adicional para esta decisión: Apple podría estar buscando fortalecer su propio ecosistema publicitario, lo que implicaría reducir la dependencia de las plataformas de terceros como Facebook y Google.

App Tracking Transparency (ATT), o Transparencia de Seguimiento de Aplicaciones, es el nombre que recibe el sistema que Apple introdujo en su versión del sistema operativo iOS 14.5. Este sistema permite a los usuarios decidir si dan permiso o no a las aplicaciones de terceros para recabar información de uso mientras utilizan las aplicaciones. Anteriormente, estas aplicaciones recopilaban datos por defecto, pero con ATT, los usuarios tienen un mayor control sobre su privacidad y pueden optar por no ser rastreados.

Con la implementación de este sistema, Apple afirma que lo que se busca es asegurar la protección y privacidad de los datos de sus usuarios y, de esta manera, mejorar la experiencia de uso. Todo este proceso de decidir si el usuario permite o no el tratamiento de sus datos se lleva a cabo mediante una ventana emergente en el dispositivo móvil cuando se abre una aplicación por primera vez. En esta ventana queda a decisión del usuario si denegar el rastreo y cruce de información o no. Según Apple, "la privacidad es un derecho humano fundamental" y ATT refuerza este compromiso (Apple, 2021).

Previo al ATT existía el *IDFA* (identificador de publicidad del dispositivo), el cual permitía el cruce de información con terceros para registrar los datos de los dispositivos y realizar campañas de marketing dirigidas. Un ejemplo de esto es cuando se realiza una búsqueda de un producto en una aplicación, como puede ser la de Amazon, y posteriormente al ingresar en una aplicación diferente te encuentras con publicidad del mismo producto que previamente has estado buscando. El *IDFA* facilitaba a las empresas el seguimiento del comportamiento de los usuarios entre diferentes aplicaciones y sitios web, permitiendo campañas de publicidad altamente personalizadas (Graham y Haselton, 2021).

Existen cuatro situaciones posibles referentes al ATT en los dispositivos móviles y si las empresas de marketing preguntan a los usuarios sí pueden acceder a sus datos y la respuesta de los usuarios a dicha pregunta.

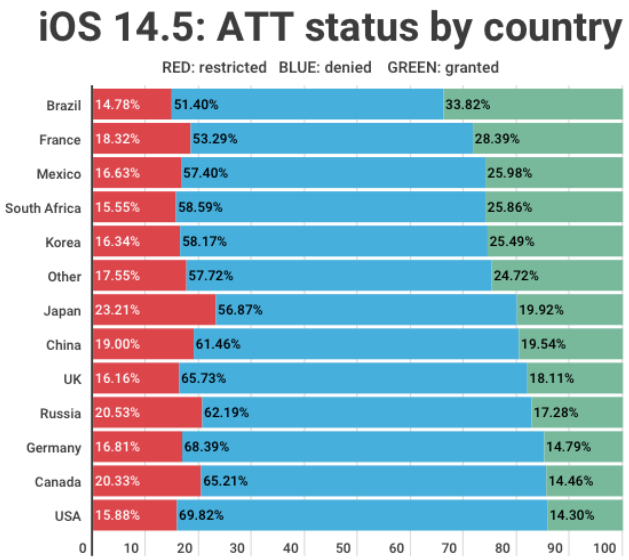
1. Restringido: los comerciantes no pueden solicitar permisos de seguimiento de datos

2. Denegado: los comerciantes pueden preguntar a los usuarios y preguntaron, pero los usuarios respondieron que no
3. Aceptado: los comerciantes preguntaron a los usuarios y estos dieron su aprobación.
4. No preguntado: los comerciantes de marketing pueden preguntar, pero aún no lo han hecho.

A continuación, se presenta una tabla que muestra la respuesta de los usuarios ante el ATT a fecha de mayo de 2021. En este gráfico, el color rojo representa a los usuarios que seleccionaron “restringido”, el color azul aquellos que seleccionaron “denegado “, y con color verde aquellos usuarios que dieron su aprobación, es decir, seleccionaron “aceptado”.

Gracias a este gráfico, podemos observar que en todos los países incluidos, más de la mitad de los usuarios de Apple de esos países han seleccionado la opción de “denegado”. Esto significa que permitieron que los comerciantes solicitaran su consentimiento para rastrear sus datos, pero estos usuarios posteriormente denegaron la solicitud.

FIGURA 3: Gráfico de respuesta de usuarios al ATT por país. Mayo 2021



Fuente: Singular (2021, Mayo 26).

Si bien es cierto que la implementación de ATT ha supuesto una desinversión inicial en publicidad en Apple y una mayor inversión en su competencia, Android, estos datos no

fueron de una gran magnitud ni se prolongaron demasiado en el tiempo. De acuerdo con un análisis de Singular (2021), aunque los anunciantes ajustaron su gasto publicitario en respuesta a la nueva normativa de privacidad, los impactos a largo plazo en el gasto publicitario no fueron tan significativos como inicialmente se temía, y el mercado publicitario se estabilizó relativamente rápido.

FIGURA 4: Inversión publicitaria por meses en Android y Apple

Fuente: Singular (2021, Mayo 26).

Como podemos apreciar en el gráfico, la mayor desinversión en publicidad en dispositivos Apple se produjo en el mes de julio, mientras que en Android sí que parece haberse mantenido en un margen previsible. Los gráficos de inversión publicitaria en teléfonos móviles a lo largo de un año suelen presentar forma de “cabeza en el centro y hombros a los laterales”, lo que refleja una fuerte inversión en los meses centrales del año, así como en los primeros y últimos meses, cuando las campañas publicitarias tienden a intensificarse debido a eventos y festividades clave.

Justo en el mes de julio, poco más de un mes después del lanzamiento de la versión 14.5, es donde se observa un pico de desinversión publicitaria en dispositivos Apple. Según una base de datos obtenida a través de aplicaciones instaladas en dispositivos Apple, que registran la versión del sistema operativo del dispositivo en el que están en uso, alrededor

del 70% de los usuarios a nivel mundial ya habían instalado la última versión disponible del sistema operativo. Hay que tener en cuenta que esta versión de software no está disponible para todos los dispositivos Apple, ya que los más antiguos van quedando obsoletos y dejan de recibir actualizaciones de software. (Koetsier, 2021)

Esta medida representa un avance significativo en la defensa de los derechos de los consumidores, ya que otorgarles la potestad de elegir sobre su información personal es un gran paso hacia la transparencia y el control de los datos. Por otro lado, limitar la capacidad de las empresas para recopilar y utilizar datos de los usuarios sin su consentimiento explícito es una acción que se debería de haber tomado hace tiempo, aunque ha perjudicado gravemente a las empresas que basan su modelo de negocio en la obtención de esta información. Para estas empresas, adaptarse a estas nuevas normativas supone un desafío considerable.

Gracias a esta nueva medida, se abren las puertas a la posibilidad de comenzar a desarrollar una manera más ética y transparente la gestión de datos de usuarios. La industria publicitaria deberá aprender a adaptarse a este nuevo entorno y depender menos del rastreo masivo de información, desarrollando nuevos métodos que ofrezcan valor tanto a los consumidores como a las empresas anunciantes (Apple, 2021; Martin y Murphy, 2016).

6.1.2. Comodidad en casa pagada con tu privacidad

Astro es un robot doméstico diseñado por Amazon, que fue lanzado al mercado en el año 2021. Se trata de un pequeño robot con ruedas que lleva incorporado una pequeña tablet y una cámara periscópica, lo que le permite, entre otras funciones, vigilar el hogar o grabar durante videollamadas. Este robot doméstico de Amazon engloba varias de las tecnologías que la empresa ha estado desarrollando y lanzando al mercado en los últimos años. Entre ellas se incluyen productos de la familia Alexa, como Alexa Together o Alexa Guard, así como dispositivos de Amazon Ring y la familia Echo, como Amazon Echo Show (Amazon, 2021).

FIGURA 5: Familia Alexa

Fuente: SmartHome News (2021).

- Alexa Together: Por una cuota, Alexa Together facilita el uso de Alexa y de los altavoces Echo tanto para asistir como para controlar a los seres queridos de avanzada edad o aquellos que necesitan un cuidador. El sistema cuenta con

detector de caídas, asistencia remota, alertas personalizadas y círculo de apoyo, entre otras. Según Amazon, “Alexa Together ayuda a los usuarios a mantenerse conectados con sus seres queridos y les brinda asistencia en caso de emergencia” (Amazon, 2021).

- Alexa Guard: Alexa Guard es una función impulsada por Alexa que utiliza los micrófonos de campo lejano que llevan integrados los dispositivos Amazon Echo para detectar sonidos sospechosos como la rotura de cristales, pasos o el sonido de las alarmas de los detectores de humo cuando estás fuera de casa. También se integra con la alarma de coche Ring para alertar de posibles robos vehiculares (Betters Picaro, 2021).

- *Ring*: se trata de una compañía de seguridad para el hogar que pertenece a Amazon. Cuenta con una amplia cartera de productos como timbres inteligentes, cámaras de seguridad y sistemas de iluminación. Estos dispositivos se conectan a la red y permiten su monitorización desde la app móvil de Ring (Ring, 2021).

- *Amazon Echo*: agrupa la familia de altavoces inteligentes de Amazon, los cuales vienen incorporados con inteligencia artificial de su asistente virtual Alexa. Los distintos modelos de Amazon Echo tienen en común micrófonos integrados, un altavoz y un control remoto. No dejan de ser un mero instrumento para ponerse en contacto con el asistente virtual Alexa. Estos dispositivos se deben conectar a la red y son capaces de reproducir música o responder a dudas que se les haga mediante los micrófonos, como hacer que cuentes chistes, te diga el tiempo o te lea las noticias (Amazon, s. f.).

- *Amazon Echo Show*: El Amazon Echo Show es un altavoz inteligente con pantalla táctil que integra el asistente virtual Alexa. La pantalla táctil permite interactuar visualmente con el dispositivo, además de por voz. Podría considerarse una evolución del Amazon Echo, ya que sus funcionalidades básicas son las mismas, pero se le incorporan varias acciones que puede realizar gracias a su pantalla de entre 5.5 hasta 10.1 pulgadas, dependiendo de la generación, como realizar videollamadas, ver recetas o reproducir videos. La pantalla varía de tamaño según la generación, de entre 5.5 a 10.1 pulgadas (CNET, 2020).

Lejos de los problemas técnicos que sufre el robot asistente de Amazon, como problemas con su cámara periscopio o que no esté preparado para subir y/o bajar escaleras, y es que, aunque en principio está diseñado para no acceder a ellas, informes recalcan que varios de

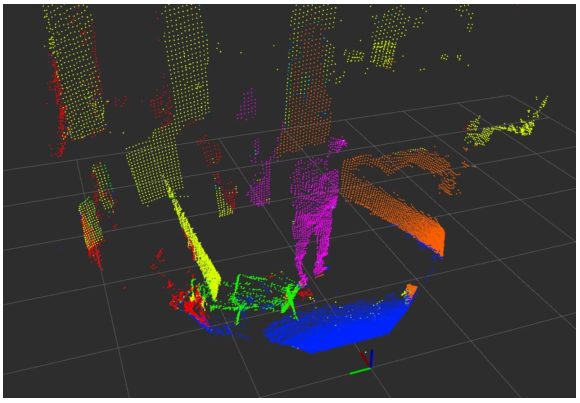
estos robots han terminado arrojándose ellos mismos escaleras abajo. Aunque, sin duda, uno de los problemas más graves y en el que nos queremos centrar más en los problemas de privacidad que genera este robot. De hecho, varios expertos han señalado que el robot Astro de Amazon plantea serias preocupaciones sobre la recopilación y manejo de datos en el hogar (Goode, 2021)."

Los propios trabajadores internos de Amazon se han atrevido a catalogar este producto como una “pesadilla de la intimidad”. Hay informes que muestran el comportamiento del “modo centinela” de Astro, el cual se activa cuando detecta una presencia humana “no registrada” en el sistema del hogar, comenzando así su función de monitorización, siguiendo al individuo a medida que emite una señal de video y audio a los teléfonos móviles de los dueños. El problema radica en que Astro no es capaz de diferenciar y reconocer a las personas que sí están registradas de las que no, por lo que actúa de la misma manera con todos los individuos, activando el modo centinela y dando fin con esto a la privacidad de los individuos (The Verge, 2021).

Aun así Amazon asegura que estos reportes se corresponden a robots que no cuentan con la última versión del sistema disponible. La empresa asegura contar con miles de horas de pruebas y ensayos en entornos beta diseñados para evitar este tipo de situaciones. Además, aseguran haber pasado controles de calidad y seguridad; además de haber revisado el sistema para que Astro sea capaz de evitar obstáculos como las escaleras que mencionamos anteriormente (Amazon, 2021). Según Amazon, estos controles garantizan que el robot esté preparado para operar en diferentes entornos sin comprometer la seguridad ni la privacidad de los usuarios.

Según Amazon Science (s. f.), “Las identidades visuales de los miembros de la casa registrados se almacenan de forma segura en el dispositivo en local” (*Privacy by Design*, párr. 1). Sin embargo, los mapas del hogar que el robot genera al pasearse por la vivienda, con el fin de mejorar su movilidad, se envían a una nube para almacenarlos. Según informa la empresa, se utilizan claves de cifrado de 256 bits para proteger los datos. Por otro lado, fuentes de la industria destacan que los documentos filtrados están desactualizados y tienen más de 12 meses, un período de tiempo "larguísimo" para el desarrollo de un producto tecnológico.

FIGURA 6: Los algoritmos de Movimiento Inteligente de Astro construyen un mapa de profundidad del entorno en el que se mueve



Fuente: Amazon (2021)

A pesar de no haber logrado hacerse un hueco en el mercado, Amazon decidió en 2023, dos años después de su debut, lanzar al mercado una nueva versión del robot Astro. Según la propia empresa, esta versión del robot está aún más destinada a la vigilancia, pero esta vez enfocado para el entorno empresarial en lugar del entorno doméstico, y nos lo hace saber mediante su nuevo seudónimo *Astro for Business*. Si bien sus funciones de vigilancia siguen siendo las mismas, el área de mapeo que puede realizar el robot ha aumentado hasta los 465 metros cuadrados, 180 metros cuadrados más que su predecesor.

Así mismo, su precio también se ha visto incrementado, en 900 dólares, alcanzando así un valor de mercado de 2.350 dólares. Sin embargo, para sacar el máximo provecho de *Astro for Business,* habrá que adquirir ciertos servicios de suscripciones mensuales, los cuales elevan su coste en 180 dólares mensuales aproximadamente (Amazon, 2023). *Astro for Business* representa una evolución en la línea de productos de Amazon, ajustándose a las necesidades de las empresas que requieren mayor seguridad y vigilancia (The Verge, 2023).

El robot Astro de Amazon realiza un procesamiento de datos en local para mapear el hogar de manera eficiente, permitiendo a los usuarios designar áreas restringidas a las que Astro no puede acceder. Para garantizar la privacidad, Astro cuenta con un piloto que se enciende para avisar cuando está grabando audio y video, especialmente durante la retransmisión en

streaming de videollamadas. Además, los usuarios pueden activar o desactivar tanto la cámara como los micrófonos en cualquier momento. Actualmente, Astro solo está disponible para su compra en los Estados Unidos (Amazon, 2021; The Verge, 2023).

¿Realmente el consumidor es consciente de la cantidad de datos que se están recopilando a cada instante? ¿Merece la pena la venta de la privacidad a cambio de comodidad? Estas son varias de las preguntas que podríamos plantearnos tras este análisis. En muchas ocasiones, los consumidores no son conscientes de la inmensa cantidad de datos personales que se están recopilando y analizando constantemente, ni el poder que estos datos otorgan a las empresas que los manejan. Según un estudio de Acquisti, Brandimarte y Loewenstein (2015), los consumidores a menudo subestiman la cantidad de información personal que están compartiendo, así como las implicaciones de esa recopilación.

Hay ocasiones en las que el consumidor prefiere vivir en la ignorancia y poder disfrutar de los lujos y las comodidades que las tecnologías nos proporcionan, sin parar a preguntarse el precio de dichos lujos. La pregunta de si vale la pena cambiar privacidad por comodidad sigue siendo un tema de debate, ya que muchos usuarios dan prioridad a la conveniencia sin considerar las posibles consecuencias a largo plazo (Tene y Polonetsky, 2013).

6.1.3. Demanda a Apple

Apple fue demandada por vender datos de sus usuarios a terceros, tal como lo señala una noticia publicada en la página web *Industriamusical* (Hernández Ruza, 2019). Tras analizar la noticia quedan latentes varias implicaciones y posibles consecuencias para la marca.

En primer lugar, esta demanda podría tener un impacto significativo en la reputación de Apple como empresa que protege la privacidad de sus usuarios. La venta de datos de usuario a terceros sin el consentimiento explícito de los usuarios puede verse como una violación de la confianza que los consumidores depositan en la marca. Esto puede repercutir en la lealtad de los clientes y afectar negativamente la imagen de marca de Apple a largo plazo. Estos aspectos negativos suelen traer consigo como repercusión una reducción en su capacidad de captación y retención de clientes. Esto debido a que nos encontramos en un mercado cada vez más competitivo y en el que los clientes dan cada vez más importancia a su privacidad (Acquisti, Brandimarte y Loewenstein, 2015).

Por otra parte, Apple ha construido su estrategia de marketing en torno a la protección de la privacidad de los usuarios. Desde la salida de sus primeros productos, muchos eran los usuarios que se inclinaban por adquirir un ordenador de esta marca en lugar de cualquier otro de sus competidores guiados por la escasez de virus informáticos y ciberataques que estos recibían. Es esta una de las razones por las que la reputación de la empresa podría verse afectada por esta arma de doble filo si se diese el caso de que se demuestra la venta de información privada a terceros sin el consentimiento explícito.

En segundo lugar, la demanda también podría tener un impacto financiero en la marca. Si bien Apple ha hecho de la privacidad de los datos una parte importante de su estrategia de marketing, como hemos mencionado anteriormente, y si se demuestra que han estado vendiendo datos de usuario a terceros, esto podría generar pérdida de ingresos y ventas en el futuro. Los consumidores que valoran la privacidad de sus datos pueden optar por elegir alternativas a Apple que ofrezcan mayores garantías en el ámbito de seguridad y transparencia, en lugar de permanecer fieles a la marca que se ha lucrado gracias a sus datos personales, lo que generaría una caída en las ventas y afectaría los beneficios de Apple (Tene y Polonetsky, 2013). "Con el aumento de las tecnologías digitales, las empresas deben equilibrar la personalización de ofertas con la protección de la privacidad del consumidor, ya que el mal manejo de los datos puede erosionar la confianza en la marca." (Kotler y Keller, 2020, p. 288).

Por otro lado, esta demanda también puede ser vista como una oportunidad para que la empresa tome medidas y restablezca la confianza de sus usuarios. En este sentido, Apple podría llevar a cabo acciones destinadas a incrementar la transparencia en la recopilación y uso de los datos de sus usuarios, así como a establecer medidas más rigurosas de seguridad para garantizar la privacidad de estos datos (Martin, Borah y Palmatier, 2017). Esto podría incluir la implementación de políticas de privacidad más claras y el anuncio público e implementación del uso de tecnologías avanzadas de seguridad de datos para evitar que terceros puedan acceder a información personal de los usuarios (Voigt y Von dem Bussche, 2017).

De esta forma, Apple podría demostrar su compromiso con la privacidad de los datos de sus usuarios, fortaleciendo su imagen de marca y recuperando la confianza de los consumidores. Una de las grandes ventajas de los dispositivos Apple es su gran ecosistema interconectado, que, en cierta medida, fomenta al usuario a estar dentro de este entorno. La gran compatibilidad entre dispositivos como los iPhone, Mac y Apple Watch genera una acumulación significativa de información sobre los usuarios y sus hábitos. Por lo tanto, es fundamental que Apple proteja adecuadamente estos datos, evitando su uso indebido para fines lucrativos, algo que los consumidores de la marca valoran positivamente (Tene y Polonetsky, 2013).

Además, este tipo de medidas también podrían proporcionar una ventaja competitiva a Apple en el mercado, ya que la privacidad de los datos se ha convertido en un tema cada vez más importante para los consumidores. Según un estudio, las empresas que priorizan la protección de datos tienen mayores probabilidades de ganar la lealtad del cliente y mejorar su posicionamiento (Martin, Borah y Palmatier, 2017). En resumen, la demanda presentada contra Apple por la venta de datos de usuarios a terceros puede ser vista como una oportunidad para que la empresa adopte medidas que incrementen la transparencia y la seguridad en el manejo de los datos personales de sus usuarios, lo que podría contribuir a recuperar la confianza de los consumidores y mejorar su posicionamiento en el mercado, a pesar de las repercusiones que tendrá de cara a su imagen de marca (Tene y Polonetsky, 2013).

En conclusión, veo esta noticia como una llamada de atención para todas las empresas que manejan datos de usuarios. La privacidad y seguridad de los datos son temas críticos que deben ser considerados y protegidos en todo momento, ya que su violación puede tener consecuencias negativas para la reputación y los ingresos de la empresa.

6.2. El marketing político y la privacidad del ciudadano:

La relación entre el marketing comercial y el marketing político ha sido objeto de análisis en diversos estudios, incluido el de Sanchís Armelles (2014). Ambos tipos de marketing comparten principios fundamentales, pero tienen finalidades diferentes. Mientras que el marketing comercial busca promocionar productos y servicios para generar ventas y satisfacer al consumidor, el marketing político está orientado a influir en la opinión pública y movilizar a los votantes para que apoyen a un candidato o partido.

En términos de estrategias, tanto en marketing comercial como en político, se emplean herramientas de comunicación persuasiva, segmentación del público objetivo, y la creación de una imagen de marca sólida. Sin embargo, el contexto de aplicación y el enfoque de las campañas son diferentes. En el ámbito político, el objetivo es captar votos y ganar elecciones, mientras que en el marketing comercial se busca la fidelización y satisfacción del cliente (Beers & Politics, s.f.).

6.2.1. Política personalizada

El marketing político es uno de los ámbitos donde se ha experimentado una mayor transformación debido al *Big Data*, ya que la recopilación masiva de datos personales permite a los partidos políticos dirigir sus mensajes de manera extremadamente precisa y personalizada. Esta práctica, que toma prestadas muchas técnicas del marketing comercial, plantea importantes desafíos en torno a la privacidad, ya no solo de los consumidores, sino que de los ciudadanos. Según Tene y Polonetsky (2013), el uso de *Big Data* en entornos políticos y comerciales expone a los usuarios a riesgos de perfilado excesivo y manipulación. Este apartado analiza cómo la segmentación de audiencias, las estrategias de marketing digital y la personalización de mensajes en el marketing político afecta la privacidad del consumidor y del ciudadano.

La segmentación de audiencias y la personalización de mensajes son unas de las técnicas clave muy utilizadas en el marketing digital; estas se usan para adaptar la comunicación, lo que se pretende transmitir, a las necesidades y preferencias específicas de cada individuo de manera personalizada. En el contexto político, estas técnicas permiten a los partidos crear perfiles detallados de los votantes; esto lo hacen basándose en su actividad en línea, como preferencias políticas, estatus socioeconómico, y otros factores personales. El artículo escrito por Gemma Galdon Clavell el 24 de marzo de 2019 para el periódico *El País* titulado “Los partidos quieren tus datos” destaca cómo los partidos políticos españoles han

aprovechado una modificación en la Ley Orgánica del Régimen Electoral General (LOREG), que les permite recopilar datos personales sin el consentimiento explícito de los ciudadanos para fines electorales, lo que incluye la realización de perfiles ideológicos y el envío de propaganda personalizada (Galdon Clavell, 2019). "Una campaña política efectiva es aquella que logra conectar emocionalmente con los votantes, ofreciendo una solución a sus problemas reales y percibidos." (Römer, 2014, p. 105), por lo que cuantos más personalizado sea el mensaje mejor resultado dará.

Esta capacidad de personalización extrema en el marketing político tiene el potencial de influir en el comportamiento electoral de manera significativa. Como afirman Hersh (2015) y Kreiss (2016), al adaptar los mensajes a los intereses y preocupaciones específicas de cada grupo de votantes, es decir, mensajes personalizados a los votantes, los partidos políticos pueden aumentar su efectividad y movilizar a electores clave. Sin embargo, también plantea riesgos considerables para la privacidad del consumidor, ya que la recopilación de datos personales a menudo se realiza sin un conocimiento adecuado por parte de los usuarios. A pesar de que en ocasiones sí se haya adquirido su consentimiento, este puede haberse adquirido de manera poco lícita o no del todo clara, lo que abre la puerta a un posible uso indebido de la información (Acquisti, Brandimarte y Loewenstein, 2015).

En el artículo de Galdon Clavell (2019) se subrayan los peligros asociados con la utilización de datos personales en el marketing político, especialmente en lo que respecta a la privacidad de los ciudadanos. Uno de los riesgos más evidentes es la invasión de la privacidad mediante la recolección y análisis de datos sin el consentimiento del individuo. La creación de perfiles detallados de votantes a partir de su actividad en línea puede resultar en una vigilancia política que limita la autonomía personal y la capacidad de los ciudadanos para tomar decisiones informadas sin influencias externas. Este tipo de prácticas puede generar una manipulación encubierta que distorsiona el proceso democrático, como advierte Zuboff (2019), quien sostiene que el *Big Data* y la recopilación masiva de datos pueden convertirse en herramientas para influir en comportamientos y decisiones políticas.

Además, el uso de datos personales para la personalización de mensajes políticos puede conducir a la manipulación del comportamiento electoral. Cuando se personalizan y ajustan los mensajes con el fin de apelar a las emociones y creencias específicas de un individuo, los partidos tienen la capacidad de manipular las percepciones y, por ello, en las decisiones de los votantes de maneras que pueden pecar de no ser siempre suficientemente transparentes o, incluso, llegar a plantear un dilema ético acerca de si son justificables o no. Esto se vuelve un tema especialmente preocupante sobre todo si tenemos en cuenta que

nos hallamos en un contexto donde los ciudadanos no tienen control sobre cómo se utiliza su información personal (Galdon Clavell, 2019).

El uso de *Big Data* en el marketing político plantea serias cuestiones éticas y legales. La recopilación de datos personales sin el consentimiento explícito de los ciudadanos no solo viola principios fundamentales de privacidad, lo cual ya resulta grave de por sí; sino que también pone en riesgo la integridad del proceso democrático en el que vivimos. La falta de regulaciones y leyes claras y la opacidad que se muestra en las prácticas de recopilación de datos dificultan que se pueda realizar una protección eficaz de la privacidad del consumidor, lo que puede resultar en abusos de poder y manipulación política a gran escala (Galdon Clavell, 2019). Según Tene y Polonetsky (2013), el uso indiscriminado de datos para influir en el comportamiento electoral no solo amenaza los derechos individuales, sino que también puede desvirtuar la confianza en el sistema democrático (Maarek, 2014, p. 192).

El artículo de Gemma Galdon Clavell también menciona el caso de Cambridge Analytica como un ejemplo de cómo el uso excesivo y descarado de datos personales puede llevar a la manipulación electoral. En este caso, la empresa utilizó datos de millones de usuarios de Facebook para desarrollar perfiles psicológicos y políticos de los votantes, que luego fueron utilizados para diseñar mensajes políticos altamente personalizados y efectivos (Galdon Clavell, 2019). Este tipo de prácticas, aunque resultan altamente eficaces desde una perspectiva de marketing, son éticamente más que cuestionables. Además, resultan legalmente arriesgadas, ya que ponen en entredicho la confianza pública en las instituciones y en el propio proceso democrático (Zuboff, 2019). La intervención de Cambridge Analytica en las elecciones de 2016, particularmente en Estados Unidos y el Reino Unido, ilustra los peligros de un uso no regulado de *Big Data* con fines políticos, lo que llevó a la desconfianza masiva en las plataformas digitales y a la intervención de los reguladores (Cadwalladr y Graham-Harrison, 2018).

El marketing político en la era del *Big Data*, tal como se describe en el artículo "Los partidos quieren tus datos" (Galdon Clavell, 2019), presenta un desafío significativo para la privacidad del consumidor y la integridad democrática. Si es verdad que la capacidad de segmentar y personalizar mensajes ofrece unas claras ventajas en cuanto a eficacia electoral se refiere, también plantea graves riesgos para la privacidad del ciudadano y la manipulación del comportamiento electoral. Como ya hemos mencionado anteriormente, según Acquisti, Brandimarte y Loewenstein (2015), la manipulación a través del uso masivo de datos puede erosionar la confianza del ciudadano en los procesos democráticos y comprometer la autonomía de sus decisiones.

Por ello, resulta de vital importancia que se desarrollen y apliquen regulaciones y leyes más estrictas que tengan como objetivo proteger los datos personales de los ciudadanos y garantizar que el marketing político se realice de manera transparente y ética. Debe garantizarse que los individuos elijan libremente su voto sin manipulaciones ni influencias externas derivada de publicidad dirigida y personalizada, siempre y cuando se quiera mantener un proceso democrático justo.

6.2.2. Facebook decide a quién debes votar

Debido a la manera en la que el marketing político ha evolucionado en los últimos años, gracias a las nuevas tecnologías que ha traído consigo la era digital y la recolección y uso masivo de datos personales que ha venido de la mano de ello, la conexión entre el marketing político y la privacidad del consumidor se ha vuelto un tema crítico. Esto se vuelve especialmente evidente después de los escándalos relacionados con la empresa Cambridge Analytica y su utilización de datos obtenidos sin el consentimiento adecuado de los usuarios de Facebook, como ya bien mencionamos anteriormente (Cadwalladr y Graham-Harrison, 2018).

El escándalo de Cambridge Analytica es un claro ejemplo de cómo el marketing político ha utilizado estrategias avanzadas de segmentación y personalización para influir en el comportamiento electoral. Según el artículo de Godoy (2020) titulado “Cambridge Analytica, la gran fuga de datos”, Cambridge Analytica recopiló datos de más de 50 millones de usuarios de Facebook sin su consentimiento explícito, para crear perfiles detallados que permitieron a campañas políticas, como la de Donald Trump en 2016, dirigir mensajes altamente personalizados y efectivos. La manera en la que la empresa adquirió los datos fue a través de una aplicación que, bajo la apariencia de un estudio académico, recopiló información personal que posteriormente fue utilizada para crear perfiles de votantes y poder dirigir mensajes políticos específicos a cada votante. Este caso remarcó la vulnerabilidad a la que se encuentran expuestos los datos personales en el entorno digital en el que vivimos y la facilidad con la que estos pueden ser manipulados para fines políticos (Cadwalladr y Graham-Harrison, 2018).

Esta práctica no solo representa una invasión a la privacidad de las personas, sino que también plantea serias preguntas sobre la ética en el marketing político. Al manipular los datos de los usuarios, se puede influir en sus decisiones políticas sin que ellos sean conscientes de la magnitud de dicha influencia. Este uso de datos cuestiona la transparencia y la equidad en los procesos democráticos, dado que el acceso a información privilegiada y la capacidad de segmentar a los votantes con un alto grado de precisión puede otorgar ventajas significativas a ciertas campañas políticas (Zuboff, 2019).

El impacto que tuvo la revelación de este suceso fue drástico, provocando una considerable pérdida de confianza en la red social culpable de esto, Facebook. Como resultado, la caída de sus acciones y una serie de investigaciones y sanciones legales a nivel global. Las Entidades públicas y gubernamentales enfatizaron la necesidad de la creación de una

regulación más estricta en la gestión de datos personales y de su uso en el ámbito del marketing político (Cadwalladr y Graham-Harrison, 2018).

Si bien Facebook es una de las plataformas digitales más grandes e influyentes a nivel global, esto también ha hecho que se haya visto situada en el centro de numerosas polémicas relacionadas con la privacidad y la desinformación. Su papel como centro de propagación de noticias falsas y de difusión de discursos de odio durante procesos electorales resulta clave, como las elecciones presidenciales de EE. UU. en 2016, mencionadas previamente, las cuales son solo uno de varios escándalos que han cuestionado el manejo de la información de los usuarios por parte de la red social fundada por Mark Zuckerberg. La compañía ha sido criticada por no tomar medidas adecuadas para proteger la privacidad de sus usuarios y por permitir que su plataforma fuera utilizada para manipular la opinión pública.

Desde las elecciones de 2016, Facebook también ha sido acusada por ser un portal donde, en cierta manera, permite la propagación de noticias falsas y discursos de odio, problemas que aún persisten y que la compañía ha intentado mitigar con nuevas políticas de control de contenido pero que aun así persisten.

El escándalo de Cambridge Analytica no sólo reveló la existencia de numerosas fallas en el sistema de protección de datos, sino que también destacó la necesidad de una mayor responsabilidad y regulación en el manejo de la información personal por parte de las grandes plataformas digitales. Esto es especialmente relevante en las redes sociales, ya que son sitios donde los usuarios, muchas veces de manera inconsciente, publican gran cantidad de información sensible sin tener en cuenta la repercusión que esta puede tener y lo mucho que les puede llegar a afectar a ellos personalmente (Cadwalladr y Graham-Harrison, 2018).

Las respuestas de Facebook, incluyendo la comparecencia de Mark Zuckerberg ante el Senado de los EE. UU. y la Eurocámara, reflejan la verdadera magnitud del problema y la presión pública que existe para mejorar las políticas de privacidad y transparencia en la gestión de datos personales de los consumidores. Además, la exposición mediática de este caso ha sensibilizado al público acerca de los peligros del uso indebido de la información personal en las plataformas digitales, lo que ha llevado a demandas de mayor responsabilidad por parte de las empresas tecnológicas y una mayor conciencia de los usuarios sobre la información que comparten en línea (Isaak y Hanna, 2018).

El auténtico desafío para las compañías que basan su modelo de negocio en la publicidad dirigida radica en equilibrar la rentabilidad de este modelo de negocio con la protección de los datos personales. La recolección y análisis de datos permite a los anunciantes, incluyendo a los factores políticos, dirigir campañas extremadamente precisas y personalizadas. Sin embargo, cuando estas prácticas se realizan sin el consentimiento informado de los usuarios, se vulnera su privacidad, generando un dilema ético y legal que las empresas tecnológicas deben resolver en la mayor brevedad posible (Isaak y Hanna, 2018).

El uso de datos personales en el marketing político plantea un dilema ético importante. Si bien las tecnologías de segmentación pueden mejorar la eficiencia y la efectividad de las campañas, también es esencial garantizar que estas prácticas se lleven a cabo de manera transparente y con el consentimiento informado de los consumidores. Según Tene y Polonetsky (2013), el equilibrio entre innovación y la protección de la privacidad es crucial en un entorno digital donde los datos se recopilan y procesan masivamente.

La protección de la privacidad debe ser una prioridad tanto para las empresas tecnológicas como para los profesionales del marketing, quienes deben equilibrar la innovación con la responsabilidad ética (Acquisti, Brandimarte y Loewenstein, 2015).

En conclusión, el análisis de esta situación muestra que el marketing político ha cruzado la línea de lo éticamente correcto al explotar datos personales sin el debido consentimiento, poniendo en riesgo tanto la privacidad de los consumidores como la integridad de los procesos democráticos. Este caso subraya la importancia de una regulación más estricta y la necesidad de adoptar prácticas más responsables en la gestión de datos personales en el marketing para proteger a los usuarios y garantizar que el marketing político no erosione los principios democráticos ni la confianza del público en las plataformas digitales a la vez que se destaca la importancia de una mayor transparencia y responsabilidad por parte de las empresas tecnológicas en el manejo de datos personales de los consumidores.

6.2.3. Google frente al Reglamento Europeo

El marketing político ha evolucionado con la llegada de las plataformas digitales como Google, las redes sociales y el *Big Data*. Estos avances permiten a los partidos políticos influir en los procesos electorales y legislativos de manera más precisa y segmentada, a la vez que se usan como herramientas para que los mensajes políticos que pueden influir de manera significativa en el comportamiento electoral y llegar a un mayor número de usuarios. Sin embargo, esta evolución también ha traído consigo riesgos y desafíos en cuanto a la transparencia y la regulación de estas prácticas.

En el artículo "Google atasca la ley europea de propaganda política "online" del periódico *El País*, Peirano (2023) destaca la tensión entre la necesidad de una regulación más estricta de la publicidad política en la Unión Europea (UE) y los esfuerzos de empresas como Google para proteger sus intereses comerciales. La Unión Europea ha intentado abordar estos desafíos mediante la propuesta de un reglamento que tenía como finalidad controlar la propaganda política en línea. Sin embargo, empresas y compañías influyentes como Google han sido acusadas de intentar frenar estas iniciativas. Esto resalta las tensiones entre la libertad de expresión, la regulación de contenidos y la protección de la privacidad del consumidor, o en este caso los ciudadanos (Peirano, 2023).

A continuación se va a proceder a analizar la influencia del reglamento de la UE en el marketing político, centrándose en las estrategias de Google para mitigar su impacto. El Parlamento Europeo, consciente de los peligros asociados con las campañas políticas poco éticas y la desinformación, ha estado trabajando en un reglamento que busca aumentar la transparencia en la publicidad política en línea. Este reglamento propone que cualquier mensaje que sea susceptible de influir en los resultados de unas elecciones, referendos o procesos legislativos esté sujeto a los mismos requisitos de transparencia que las comunicaciones pagadas por partidos políticos (European Commission, 2021).

Específicamente, la legislación exige que todos los anuncios políticos incluyan detalles sobre su coste, quién los diseñó, y a qué audiencia están dirigidos (Peirano, 2023). Este enfoque busca combatir las llamadas "campañas políticas oscuras", que han sido utilizadas en eventos clave como el *Brexit* y las elecciones presidenciales en Estados Unidos, de las que ya hemos hablado anteriormente. Estas campañas suelen basarse en el uso no autorizado de datos personales para crear mensajes altamente personalizados que son enviados de manera encubierta a ciudadanos seleccionados especialmente para ello, lo

cual tira por los suelos todo principio de transparencia y equidad en los procesos democráticos (Peirano, 2023).

Google, como una de las principales plataformas utilizadas para la difusión de publicidad política, ha reaccionado a estas propuestas legislativas con resistencia. La empresa ha desplegado una estratégica campaña para influir en la opinión de los europarlamentarios y evitar, o al menos tratar de frenar, el avance de implementación de esta regulación. Google argumenta que el reglamento podría limitar la libertad de expresión política en las redes al comparar y tratar por igual el discurso político no remunerado y la publicidad política pagada (Peirano, 2023).

Con el fin de reforzar su argumento, Google ha utilizado organizaciones como DOT Europe, una asociación que representa a grandes plataformas digitales, y ha involucrado a *youtubers* e *influencers* para presionar a los legisladores, sugiriendo que sus contenidos podrían ser censurados bajo esta nueva ley. Mediante estas tácticas se busca generar preocupación entre los creadores de contenido y, a su vez, entre los europarlamentarios, al enfatizar los posibles efectos no deseados que el reglamento podría tener sobre la libertad de expresión en el entorno digital (European Commission, 2021; Peirano, 2023).

DOT Europe es una asociación que representa a las principales empresas de internet en Europa, tales como Google, Amazon y Apple. Su objetivo es promover que internet sea un lugar innovador, abierto y seguro tanto para los usuarios y consumidores como para las empresas que se encuentran y operan en él. Este objetivo pretende cumplirlo influyendo en la política digital de la Unión Europea. DOT Europe además participa activamente en la creación y desarrollo de propuestas regulatorias que tengan que ver con temas como la privacidad, la inteligencia artificial y el mercado digital (DOT Europe, 2024).

Sin embargo, tal y como se menciona en el artículo “Google atasca la ley europea de propaganda política online” del periódico *El País*, este argumento de Google no es del todo preciso. La regulación no busca restringir la libertad de expresión, sino asegurar que la publicidad política pagada sea transparente y se identifique claramente como tal, permitiendo que los usuarios también puedan identificarlas fácilmente (Peirano, 2023). El verdadero objetivo de la ley es que las plataformas digitales se responsabilicen de la difusión de campañas de influencia que son amplificadas por sus algoritmos, especialmente aquellas que se promocionan de manera "inauténtica" y que no se identifican como publicidad política.

Aunque Google sostiene que defiende la libertad de expresión, el artículo de Peirano sugiere que la verdadera motivación de la empresa es evitar la responsabilidad que implicaría la aplicación de las nuevas regulaciones, especialmente en lo que respecta al control de los algoritmos de recomendación que conciernen al contenido político dirigido (Peirano, 2023). Estos algoritmos pueden amplificar mensajes políticos sin la transparencia requerida, lo que genera un debate sobre la necesidad de regular las plataformas para garantizar la equidad en los procesos electorales (European Commission, 2021).

La intervención y postura de Google en este debate contra el reglamento de la UE resalta las tensiones ya existentes entre las prácticas comerciales de las grandes plataformas y la necesidad de proteger la integridad del proceso democrático, a la vez que plantea preguntas sobre la transparencia en el marketing político y sobre la privacidad del consumidor. El marketing político digital, si bien permite una segmentación precisa y una mayor eficacia en la comunicación, también puede llevar a abusos que erosionan la confianza pública en las instituciones democráticas (Zuboff, 2019).

Los algoritmos de Google están diseñados para recopilar grandes cantidades de datos personales con el fin de personalizar y dirigir publicidad en términos generales, lo cual incluye la publicidad política. La falta de transparencia en cómo se manejan estos datos y cómo se utilizan para influir en los votantes es una de las preocupaciones más importantes. Si las plataformas como Google no están obligadas a revelar cómo se amplifican y segmentan los mensajes políticos, los consumidores corren el riesgo de ser manipulados sin ser conscientes de la influencia a la que están siendo sometidos (Peirano, 2023). La falta de transparencia en la publicidad política no solo afecta igualdad de oportunidades en las elecciones, sino que también puede violar la privacidad de los ciudadanos al utilizar sus datos personales sin un consentimiento adecuado (European Commission, 2021)..

Este conflicto subraya la importancia de desarrollar marcos regulatorios que puedan adaptarse a la rápida evolución del marketing digital, sin tener que sacrificar los principios fundamentales de transparencia y privacidad. La resistencia de Google a la legislación propuesta por la UE nos demuestra cómo las grandes plataformas pueden intentar influir en las regulaciones con el fin de proteger sus modelos de negocio, a menudo sacrificando la protección de los derechos del consumidor y del ciudadano (Peirano, 2023). Sin un marco regulatorio sólido, los ciudadanos pueden ser objeto de campañas de propaganda que exploten sus datos personales, lo que no solo viola su privacidad sino que también erosiona y deteriora la confianza en el proceso democrático.

El caso de Google y el reglamento de la UE sobre publicidad política destacan la complejidad y los desafíos que enfrentan los legisladores al intentar regular un entorno digital que se encuentra en constante cambio. Mientras que las plataformas digitales han revolucionado el marketing político, también han creado oportunidades para la manipulación y la falta de transparencia. La necesidad de una regulación eficaz que proteja tanto la privacidad de los ciudadanos como la integridad de los procesos electorales es más urgente que nunca. Cada vez es más importante que los marcos regulatorios avancen y no se enfoquen únicamente en la transparencia, sino que también responsabilicen a las plataformas digitales de su papel en la difusión de contenidos políticos, asegurando que el marketing político digital se realice de manera ética y conforme a los principios democráticos, protegiendo tanto la privacidad del ciudadano como la equidad en el proceso electoral.

6.2.4. Tus datos a cambio de un billete de lotería

El caso presentado en la noticia “la gran rifa de Alvise” difundida por el periódico *El País* (Gonzalez, 2024), supone un claro ejemplo de cómo se relacionan el marketing, la política y la privacidad de los consumidores o de los ciudadanos entre sí. Alvise Perez, actual eurodiputado del partido político Se acabó la Fiesta (SALF), utilizó como reclamo para ganar votantes la promesa de sortear su sueldo como eurodiputado. Lo que en un principio parecía una mera estrategia de captación de votantes a través de un factor económico comienza a transformarse en una recolección masiva de datos personales. Este enfoque trae consigo importantes reflexiones desde el punto de vista del marketing y la privacidad, tanto en un contexto comercial como político.

Siguiendo la estrategia del actual presidente argentino Javier Milei, Alvise también prometió sortear su sueldo. La única diferencia entre estas dos personas es la manera en la que uno, Milei, realizó esta rifa y la manera en la que Alvise pretende realizar el sorteo de su sueldo como eurodiputado. Si bien Milei realizó dicho proceso ante notario, con todo lo que ello implica a nivel legal, la propuesta que Alvise ha dejado sobre la mesa es algo diferente. La propuesta de Alvise pasa por utilizar un *Smart Contract* o contrato inteligente, el cual debido a que es un sistema basado en *blockchain* podríamos considerar que se trata de un sistema fiable dentro de lo que cabe (Tapscott y Tapscott, 2016). El problema yace en los datos necesarios y requeridos para participar en este sorteo y lo que ello implica. Al exigir datos personales específicos para participar en el sorteo, como el nombre, número de teléfono, correo electrónico, y perfiles en redes sociales, se está construyendo lo que podríamos considerar como un "tesoro" de valiosa información para futuras campañas de marketing (Kitchin, 2014). Desde la perspectiva del marketing, la estrategia utilizada por Alvise Pérez es un ejemplo clásico de cómo las técnicas de recopilación de datos se pueden utilizar para construir bases de datos masivas de potenciales consumidores a un bajo costo.

La obtención de estos datos puede permitir la creación de campañas de marketing altamente segmentadas, donde los mensajes publicitarios pueden ser personalizados para cada individuo basándose en su comportamiento y preferencias, una técnica conocida como marketing dirigido (Turow, 2011), tal y como sucedió en las ya mencionadas elecciones de Estados Unidos. Sin embargo, esto plantea serios riesgos en términos de privacidad del consumidor. Tal y como señala la noticia, los datos personales recolectados no solo pueden ser utilizados para contactar a los participantes, sino que también pueden ser difundidos públicamente o vendidos a terceros sin el consentimiento explícito de los usuarios, violando así su privacidad (Zuboff, 2019).

Este tipo de prácticas refleja el fenómeno que Acquisti y Grossklags (2005) describen como una "paradoja de la privacidad", en la que los usuarios, a menudo sin darse cuenta, sacrifican su privacidad por servicios que perciben como valiosos. Además, Solove (2004) argumenta que la recolección masiva de datos personales plantea serios desafíos al control que los usuarios tienen sobre su información, un problema que se ve exacerbado por la creciente interconectividad de las redes sociales y la economía digital (Barocas y Nissenbaum, 2014).

Y es que ya se advierte en las bases legales del propio sorteo que Alvise “se reserva el derecho de modificar los términos y condiciones [del sorteo] de forma retroactiva”. Además de ello, Alvise, como responsable legal del tratamiento de los datos personales, podrá, si así lo quiere, realizar publicaciones en el perfil de cualquiera de los participantes de su sorteo. Esto le permitirá al líder de SALF exponer su publicidad política a un coste mínimo y con una gran repercusión, ya que su mensaje llegará a la gente que no le sigue a él directamente en diversas redes sociales gracias a la gente que si le sigue y tienen en común, lo cual multiplica exponencialmente la difusión de propaganda política (Andrejevic, 2013). La aceptación de estos términos es un claro ejemplo de políticas de privacidad complejas, poco claras y abusivas.

La promesa de sorteo de 8.000 euros se trata de una técnica de recopilación de datos camuflada bajo el nombre de “sueldo de eurodiputado” ya que, en realidad, no se trata de la totalidad de ingresos que el eurodiputado de SALF percibirá. Además de una retribución de 10.377,43 euros brutos mensuales, percibe una dieta por asistencia al pleno de 300 euros por pleno asistido, 27.000 euros mensuales para asistentes, aproximadamente 60.000 euros anualmente para propaganda política y 4.100 euros que tienen como destinatario gastos de oficina. Aunque es verdad que estos no se pueden sortear debido a que son lo que se consideran como partidas finalistas, a lo que sí que podría haber renunciado el eurodiputado es al sueldo de los otros dos eurodiputados de su partido político SALF que acompañan a Alvise debido a sus resultados en las elecciones, pero han decidido no hacerlo.

Es por ello que gracias al señuelo de estos 8.000 euros Alvise ya ha logrado obtener una bolsa de potenciales votantes, ya que las bases del sorteo exigen tener más de 18 años para poder participar y por ello se pueden considerar votantes potenciales. Además, ha recolectado una gran cantidad de datos personales suyos, lo cual es un intercambio más que favorable para el partido SALF, ya que dicha información vale mucho más que esos 8.000 euros a los que supuestamente está renunciando.

Este tipo de estrategias encaja dentro del fenómeno descrito por Zuboff (2019) como "capitalismo de vigilancia", en el que los datos personales de los usuarios se recopilan para ser monetizados. Según Acquisti y Grossklags (2005), los usuarios, a menudo sin darse cuenta, intercambian su privacidad por oportunidades o servicios que perciben como valiosos, mientras que Barocas y Nissenbaum (2014) advierten sobre cómo el *Big Data* ha erosionado las fronteras del consentimiento y el anonimato. Solove (2004) señala que la creciente acumulación de datos plantea importantes preocupaciones sobre la privacidad y el control individual en la era digital, lo cual se ve reflejado en este tipo de prácticas donde los partidos políticos, como SALF, pueden obtener valiosos datos personales a un bajo costo financiero.

En el ámbito político, el uso de estas técnicas de recopilación de datos se ha vuelto cada vez más común, como lo demuestra la estrategia de Alvise Pérez. La creación de una base de datos con millones de registros de posibles votantes permite a los partidos políticos segmentar a su audiencia y dirigir mensajes específicos que pueden influir en la opinión pública y en los resultados electorales. Esta técnica es un ejemplo de cómo el marketing político ha evolucionado, utilizando estrategias similares a las empleadas en el marketing comercial (Kreiss, 2016).

Sin embargo, la privacidad del ciudadano se ve altamente afectada por este proceso. Los participantes del sorteo, que posiblemente no son conscientes del alcance del uso de los datos que ellos mismos han regalado, podrían verse expuestos a un bombardeo de mensajes y campañas políticas, los cuales tendrán como objetivo tratar de manipular sus preferencias y comportamientos. Este tipo de marketing político, que se aprovecha de tener a su disposición grandes volúmenes de datos, puede llegar a influir en las decisiones políticas de los ciudadanos de manera sutil, pero significativa, deteriorando la libre elección y la privacidad del individuo (Kreiss, 2016).

El caso de "La gran rifa de Alvise" pone en evidencia la delgada línea entre las oportunidades y los riesgos que trae la Revolución Digital en términos de marketing y privacidad. Mientras que las técnicas de recolección de datos pueden generar beneficios significativos tanto para empresas como para partidos políticos, se vuelve esencial considerar las implicaciones éticas y legales que conllevan, especialmente en lo que respecta a la protección de la privacidad de los consumidores y ciudadanos. En este contexto, es fundamental que existan regulaciones claras y que los consumidores estén informados y protegidos frente a prácticas que puedan vulnerar su derecho a la privacidad y

que sean conscientes en todo momento del tratamiento que tendrán los datos que proporcionen.

7. Conclusiones

La sociedad en la que vivimos ha sufrido enormes cambios debido a la Revolución Digital. Esta era digital en la que vivimos nada tiene que ver con la vida de años atrás. Ha cambiado la economía, mediante la creación de nuevos modelos de negocio y facilitando una economía más global y automatizada, con la creación de multitud de portales en línea donde consumidores pueden acceder a productos de cualquier parte del mundo desde la comodidad de su casa con el único requisito de tener acceso a internet. También ha cambiado la manera en la que trabajamos, facilitando trabajos ya existentes gracias a la automatización de procesos productivos y creando múltiples nuevos puestos de trabajo basados en las tecnologías. Pero, sobre todo, se ha visto alterado la manera en la que nos comunicamos. Con la llegada de internet a la vida cotidiana, el fácil acceso a él y las pocas barreras de entrada que presenta la obtención de dispositivos que nos permitan tener acceso a él, ha cambiado drásticamente la manera en la que el ser humano se comunica. Desde la creación de internet, su propósito ha sido facilitar la comunicación entre usuarios, y esto ha ido progresando y evolucionando hasta la multitud de portales sociales que existen hoy en día.

Todos estos avances son claramente beneficiosos para las personas, pero como todo tiene su contraparte, y es que a cada nuevo avance emergente se presentan una serie de nuevos retos que hay que afrontar. Debido a la automatización de tareas productivas, han quedado puestos de trabajo obsoletos, lo cual, si para las empresas puede presentar beneficios en forma de ahorro de sueldos y salarios, hace que haya personas que hayan perdido sus empleos. Con la llegada de los portales en línea y la facilidad de poder comprar en cualquier momento y en cualquier lugar, así como de comparar productos en línea, ha afectado a los pequeños comercios que, en ocasiones, no pueden soportar la guerra de precios que grandes portales en línea pueden manejar con buenos márgenes debido a una mejor logística. Además, con la llegada de las redes sociales, la privacidad de los usuarios ha quedado en segundo plano debido a la cantidad de datos personales que quedan expuestos en estos portales.

Cada vez que realizamos un *post* en una red social, cada vez que compramos un producto o contratamos un servicio en línea, cada vez que nos registramos en una nueva página web, e incluso cada vez que realizamos una búsqueda en un motor de búsqueda, o cada vez que aceptamos las cookies de una página web, estamos dejando una huella digital que permanece y es imperecedera. En muchas ocasiones, depositamos estos datos

conscientemente, como al dejar nuestra dirección para que nos puedan entregar un pedido en línea; y en otras, muchas de manera inconsciente, como cuando haces clic en un artículo de un portal en línea para verlo mejor o más detalladamente. En otras ocasiones, simplemente permitimos que recopilen datos sobre nuestro comportamiento sin llegar a ser plenamente conscientes de que tipo de datos se van a recopilar o con qué fin se van a utilizar, ya sea porque no leemos los términos y condiciones de uso o porque estos no sean lo suficientemente claros y concisos. A su vez, todos estos datos deben estar debidamente salvaguardados por las compañías que los almacenen debido a su importancia.

Si bien toda la información que vamos dejando en internet en distintos portales puede ser poca y parecer inofensiva, sirve para poder crear un perfil de consumidor, lo cual presenta ventajas y desventajas. A una persona que tenga un perro como mascota y que tiende a comprar productos para perros en línea, le puede ser de utilidad que la publicidad que vea mientras está navegando por internet tenga que ver con perros, ya sea comida, accesorios o cursos de adiestramiento. Sin embargo, de poco le servirán anuncios de comida para gatos. Por otra parte, este tipo de publicidad personalizada limita en cierta manera la libre elección del consumidor. Cuando este ejemplo lo extrapolamos a otros ámbitos, como el político, puede llegar a tener graves consecuencias.

Resulta imperante la necesidad de una legislación y regulación que proteja a los consumidores frente a políticas abusivas y garantice su privacidad y bienestar digital. Todo avance debe ir debidamente acompañado de una garantía de seguridad para los usuarios y consumidores. No podemos permitir que las grandes organizaciones se lucren a costa de nuestra privacidad y que lo hagan con total libertad, sin restricciones ni penalizaciones.

Para los partidos políticos, internet no es únicamente el lugar donde hacer publicidad para poder llegar a un gran número de personas de una manera más económica que mediante medios convencionales. Es una manera de conocer la situación en la que se encuentra su partido; es una ventana al mundo. Además, no se puede persuadir a quien no se conoce, por lo que, para influir en los votantes, primero hace falta conocerlos bien. Los partidos buscan apelar a nuestros sentimientos y emociones, ya que así es como consiguen votos. Los ciudadanos votamos por proximidad y por sentimientos (Sanchís, 2014). Los estrategas electorales son conscientes de que lo que hace a los ciudadanos elegir a quién votar son el miedo (que provoca rechazo) y la esperanza (que provoca ilusión). Una vez que hayan logrado convencernos emocionalmente, esperan que seamos los propios ciudadanos quienes actuemos como altavoces de sus propuestas e ideales.

Podemos considerar a los ciudadanos y a los consumidores como las dos caras de la misma moneda, como ya expresó Bauman (2007) en su libro *Consumo, luego existo*. Tanto para las empresas como para los partidos políticos, las personas no somos más que simples números que creen tener el derecho de manipular para lograr sus objetivos. Para unos, somos consumidores que les permiten alcanzar el nivel de ventas deseado. Para los otros, un número más que necesitan para que creamos en ellos y en sus promesas, con el fin de obtener poder a través de nuestro voto. Pero ambos están tratando de venderte algo, ya sea un producto o un candidato. Nos consideran una herramienta que pueden usar a su antojo, intentando manipularnos y, en muchas ocasiones, atentando contra nuestra privacidad y privándonos de la libertad de elección que deberíamos tener.

Nuestro deber como consumidores es ser conscientes de los datos e información personal que dejamos al navegar por internet y de cómo las empresas y organizaciones pueden hacer uso de ellos. Por otro lado, las empresas tienen la responsabilidad de conservar debidamente estos datos y hacer un buen uso de ellos. Nuestros datos personales no son una mercancía con la que las empresas puedan negociar y obtener beneficios de ello.

Como reflexión final, deberíamos plantearnos la siguiente pregunta: ¿qué somos para las empresas y los partidos políticos? ¿No somos más que un medio para alcanzar un fin? ¿Votos, ventas... es lo mismo? Al final, parece que lo único que buscan de nosotros son números, y así es como nos ven: como un número más al que llegar emocionalmente, sin que realmente les importen nuestras emociones (irónicamente).

8. Bibliografía

Accenture. (2018, 3 de mayo). Widening Gap Between Consumer Expectations and Reality in Personalization Signals Warning for Brands, Accenture Interactive Research Finds. https://newsroom.accenture.com/news/2018/widening-gap-between-consumer-expectations-and-reality-in-personalization-signals-warning-for-brands-accenture-interactive-research-finds

Acquisti, A., y Grossklags, J. (2005). Privacy and rationality in individual decision making. IEEE Security & Privacy, 3(1), 26-33. https://doi.org/10.1109/MSP.2005.22

Acquisti, A., Brandimarte, L., y Loewenstein, G. (2015). Privacy and human behavior in the age of information. Science, 347(6221), 509-514. doi:10.1126/science.aaa1465

Adomavicius, G., y Tuzhilin, A. (2005). Personalization technologies: A process-oriented perspective. Communications of the ACM, 48(10), 83-90. doi:10.1145/1089107.1089109

Allcott, H., y Gentzkow, M. (2017). Social media and fake news in the 2016 election. Journal of Economic Perspectives, 31(2), 211-236. doi:10.1257/jep.31.2.211

Amazon Science. (s. f.). Privacy by Design. Amazon Science. https://www.amazon.science

Amazon. (2021). Amazon responds to Astro privacy concerns. Amazon.com. https://www.amazon.com

Amazon. (2021). Introducing Alexa Together: Stay connected with loved ones, and get help when needed. Amazon.com. https://www.amazon.com/newsroom

Amazon. (2021). Meet Astro, household robot for home monitoring. Amazon.com. https://www.amazon.com/Astro

Amazon. (2021). The science behind visual ID. Amazon Science. https://www.amazon.science/blog/the-science-behind-visual-id

Amazon. (2023). Introducing Astro for Business: Security and monitoring reimagined. Amazon.com. https://www.amazon.com

Amazon. (s. f.). Alexa Guard. https://www.amazon.com/alexa-guard

Anderson, R., y Moore, T. (2006). The economics of information security. Science, 314(5799), 610-613. https://doi.org/10.1126/science.1130992

Andrejevic, M. (2002). The work of being watched: Interactive media and the exploitation of self-disclosure. Critical Studies in Media Communication, 19(2), 230-248.

Andrejevic, M. (2011). Surveillance and alienation in the online economy. Surveillance & Society, 8(3), 278-287. https://doi.org/10.24908/ss.v8i3.4164

Andrejevic, M. (2013). Infoglut: How too much information is changing the way we think and know. Routledge.

Apple. (2021). User privacy and data use: App Tracking Transparency. Apple Inc. https://www.apple.com/newsroom

Barocas, S., y Nissenbaum, H. (2014). Big data's end run around anonymity and consent. In J. Lane, V. Stodden, S. Bender, y H. Nissenbaum (Eds.), Privacy, Big Data, and the Public Good: Frameworks for Engagement (pp. 44-75). Cambridge University Press. https://doi.org/10.1017/CBO9781107590205.004

Bauman, Z. (2007). Consumo, luego existo. Fondo de Cultura Económica.

Bawden, D., y Robinson, L. (2009). The dark side of information: Overload, anxiety and other paradoxes and pathologies. Journal of Information Science, 35(2), 180-191. https://doi.org/10.1177/0165551508095781

Beers & Politics. (s. f.). Elementos básicos de una campaña electoral. https://beersandpolitics.com

Betters Picaro, E. (2021, 27 de septiembre). What is Alexa Guard and how does it work? Pocket-lint. https://www.pocket-lint.com/smart-home/news/amazon/148044-what-is-alexa-guard-and-how-does-it-work/

Betters Picaro, E. (2021, 7 de diciembre). Amazon Alexa Together: Price, features, and how does it work? Pocket-lint. https://www.pocket-lint.com/smart-home/news/amazon/159324-amazon-alexa-together-price-features-how-does-it-work/

Brynjolfsson, E., Hu, Y. J., y Rahman, M. S. (2013). Competing in the age of omnichannel retailing. MIT Sloan Management Review, 54(4), 23-29.

Brynjolfsson, E., y McAfee, A. (2014). The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies. W.W. Norton & Company.

Business Insider. (2021). Facebook warns Apple's iOS 14 update will harm its advertising business. Business Insider. https://www.businessinsider.com/facebook-warns-ios-14-apple-privacy-update-harm-advertising-business-2021

Button, M., Nicholls, C. M., Kerr, J., y Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. Australian & New Zealand Journal of Criminology, 47(3), 391-408. https://doi.org/10.1177/0004865814521224

Buzzard, J., y Kitten, T. (2021, 23 de marzo). 2021 identity fraud study: Shifting angles. Javelin Strategy & Research. https://www.javelinstrategy.com/research/2021-identity-fraud-study-shifting-angles

Cadwalladr, C., y Graham-Harrison, E. (2018, marzo 17). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian. https://www.theguardian.com

Castells, M. (2010). La sociedad red: una visión global. Enl@ ce: revista venezolana de información, tecnología y conocimiento, 7(1), 139-141.

Cavallo, A. (2017). Are online and offline prices similar? Evidence from large multi-channel retailers. American Economic Review, 107(1), 283-303. doi:10.1257/aer.20160542

Chevalier, J. A., y Mayzlin, D. (2006). The effect of word of mouth on sales: Online book reviews. Journal of Marketing Research, 43(3), 345-354. https://doi.org/10.1509/jmkr.43.3.345

Clark, M. (2021, 28 de septiembre). Amazon Astro es frágil, malo en las escaleras y se lanzará por ellas si se le da la oportunidad, afirman documentos de desarrolladores. The Verge. https://www.theverge.com/2021/9/28/22699284/amazon-astro-real-world-stairs-fragile-developer-claims-documents-tracking

Clark, M. (2021, 29 de septiembre). Amazon Astro is "terrible" and will "throw itself down" stairs, developers reportedly claim. The Verge. https://www.theverge.com/2021/9/28/22699284/amazon-astro-real-world-stairs-fragile-developer-claims-documents-tracking

CNET. (2020). Amazon Echo Show: Smart displays with Alexa. CNET. https://www.cnet.com

Comisión Federal de Comercio de Estados Unidos. (2020). Consumer Sentinel Network Data Book 2020. Recuperado de https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2020

Deloitte. (2023). Consumer data privacy and security: Concerns over data privacy on smart devices. Deloitte Insights. https://www2.deloitte.com

DOT Europe. (2024). About us. https://doteurope.eu

Eppler, M. J., y Mengis, J. (2004). The concept of information overload: A review of literature from organization science, accounting, marketing, MIS, and related disciplines. The Information Society, 20(5), 325-344. doi:10.1080/01972240490507974

Eslami, M., Rickman, A., Vaccaro, K., Aleyasen, A., Vuong, A., Karahalios, K., Hamilton, K., y Sandvig, C. (2015). "I always assumed that I wasn't really that close to [her]": Reasoning about invisible algorithms in news feeds. Proceedings of the 2015 ACM CHI Conference on Human Factors in Computing Systems, 153-162. doi:10.1145/2702123.2702556

Espinoza, J. (2021, 26 de abril). German groups file Apple antitrust complaint as it makes privacy changes. *Financial Times*. https://www.ft.com/content/0a48d9aa-244b-4945-b2a0-01c68683544a

European Commission. (2021). Proposal for a Regulation on the transparency and targeting of political advertising. https://ec.europa.eu

Europol. (2020). Internet Organised Crime Threat Assessment (IOCTA) 2020. https://www.europol.europa.eu/iocta-report

Federal Trade Commission (FTC). (2020). Consumer Sentinel Network Data Book 2020. https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2020

Flavián, C., Gurrea, R., y Orús, C. (2016). Choice confidence in the webrooming purchase process: The impact of online positive reviews and the motivation to touch. Computation and Chemistry, 40(1), 1-15. https://doi.org/10.1002/cb.1585

Flores, C. (2019, 25 de febrero). Así es Ring, la compañía de seguridad para el hogar de Amazon. El Economista. https://www.eleconomista.es/tecnologia/noticias/9721887/02/19/asi-es-ring-la-compania-de-seguridad-para-el-hogar-de-amazon.html

Galdon Clavell, G. (2019, marzo 24). Los partidos quieren tus datos. *El País.* https://elpais.com

GAME España. (2024). Página principal. GAME. https://www.game.es/

Gault, M., y Cox, J. (2021, 28 de septiembre). Leaked documents reveal Amazon Astro's potential for surveillance and tracking. Vice. https://www.vice.com/en/article/93ypp8/leaked-documents-amazon-astro-surveillance-robot-tracking

Gault, M., y Cox, J. (2021, 28 de septiembre). Leaked documents show Amazon's Astro robot is a surveillance nightmare. Vice. https://www.vice.com/en/article/93ypp8/leaked-documents-amazon-astro-surveillance-robot-tracking

Gillis A.S. (2022). Gig economy (economía de trabajos esporádicos). TechTarget. https://www.techtarget.com/whatis/definition/gig-economy

Godoy, J. D., y Bueno, O. L. (2020). Cambridge Analytica, la gran fuga de datos. *El País*.

Godoy, J. D., y Bueno, O. L. (2020). Facebook: cuatro años en el centro de la polémica. *El País.*

Goldfarb, A. y Tucker, C. E. (2011). Online display advertising: Targeting and obtrusiveness. Marketing Science, 30(3), 389-404. https://doi.org/10.1287/mksc.1100.0583

González, M. (2024, 15 de agosto). La gran rifa de Alvise, un tesoro de millones de datos personales por 8.000 euros al mes. *El País.*

González, M. (2024, 15 de agosto). La gran rifa de Alvise: un tesoro de millones de datos personales por 8,000 euros al mes. *El País*. https://elpais.com/espana/2024-08-15/la-gran-rifa-de-alvise-un-tesoro-de-millones-de-datos-personales-por-8000-euros-al-mes.html

Goode, L. (2021, 28 de septiembre). Amazon's Astro is a home robot with a lot of potential—and a lot of questions. Wired. https://www.wired.com/story/amazon-astro/

Google. (2023, Julio). Llega a clientes cautos que tienen nuevos valores. Think with Google. https://www.thinkwithgoogle.com/intl/es-419/estrategias-de-marketing/experiencia-de-compra/guia-retail-latam-2023/

Graham, M., y Haselton, T. (2021, 26 de abril). Apple's iOS 14.5 update gives users more control over app tracking. CNBC. https://www.cnbc.com/2021/04/26/apple-ios-14point5-iphone-update-app-tracking-feature.html

Gupta, S., Lehmann, D. R., y Stuart, J. A. (2004). Valuing customers. Journal of Marketing Research, 41(1), 7-18. https://doi.org/10.1509/jmkr.41.1.7.25084

Hernández Ruza, J. (2019). Apple es demandada por vender datos de sus usuarios a terceros. https://industriamusical.com/apple-es-demandada-por-vender-datos-de-sus-usuarios-a-terceros/

Hernández, G. (2021, 30 de septiembre). Documentos filtrados dicen que Astro es una pesadilla para la privacidad; Amazon asegura que pasó todas las pruebas de calidad. Xataka. https://www.xataka.com.mx/accesorios/documentos-filtrados-dicen-que-astro-pesadilla-privacidad-amazon-asegura-que-paso-todas-pruebas-calidad

Hersh, E. D. (2015). Hacking the electorate: How campaigns manipulate voters' preferences and behaviors. Cambridge University Press.

Hilbert, M. (2011). The end justifies the definition: The manifold outlooks on the digital divide and their practical usefulness for policy-making. Telecommunications Policy, 35(8), 715-736. https://doi.org/10.1016/j.telpol.2011.06.012

Holgado, R. (2021, 29 de septiembre). Astro, el nuevo robot de videovigilancia de Amazon, vulnera la privacidad del cliente según un documento filtrado. 20 Minutos. https://www.20minutos.es/tecnologia/ciberseguridad/astro-el-nuevo-robot-de-videovigilancia-de-amazon-vulnera-la-privacidad-del-cliente-segun-un-documento-filtrado-4837776/

HubSpot. (2024). The Ultimate List of Marketing Statistics for 2022. HubSpot. https://www.hubspot.com/marketing-statistics

IAB. (2019). IAB Internet Advertising Revenue Report 2019. Interactive Advertising Bureau. https://www.iab.com/wp-content/uploads/2020/05/FY19-IAB-Internet-Ad-Revenue-Report_Final.pdf

Iberdrola. (s. f.). ¿Qué es el machine learning? https://www.iberdrola.com/innovacion/machine-learning-aprendizaje-automatico

Isaak, J., y Hanna, M. J. (2018). User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. Computer, 51(8), 56-59. https://doi.org/10.1109/MC.2018.3191268

Jenkins, H. (2006). Convergence culture: Where old and new media collide. New York University Press.

Kaplan, A. M., y Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. Business Horizons, 53(1), 59-68. doi:10.1016/j.bushor.2009.09.003

Kitchin, R. (2014). The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences. SAGE.

Koetsier, J. (2021, 4 de junio). iOS 14.5 by the numbers: Adoption, ATT permission, ad spend trends, install volume impact on Android vs iOS. Singular. https://www.singular.net/blog/ios-14-5-by-the-numbers-adoption-att-permission-ad-spend-trends-install-volume-impact-on-android-vs-ios/

Kotler, P., y Keller, K. L. (2020). Marketing management (15th ed.). Pearson.

Kreiss, D. (2016). Prototype politics: Technology-intensive campaigning and the data of democracy. Oxford University Press.

Kumar, V., y Shah, D. (2009). Expanding the role of marketing: From customer equity to market capitalization. Journal of Marketing, 73(6), 119-136. https://doi.org/10.1509/jmkg.73.6.119

Lazer, D. M., Baum, M. A., Benkler, Y., Berinsky, A. J., Greenhill, K. M., Menczer, F., ... y Zittrain, J. L. (2018). The science of fake news. Science, 359(6380), 1094-1096. https://doi.org/10.1126/science.aao2998

Leeflang, P. S. H., Verhoef, P. C., Dahlström, P., y Freundt, T. (2014). Challenges and solutions for marketing in a digital era. European Management Journal, 32(1), 1-12. https://doi.org/10.1016/j.emj.2013.12.001

Lewandowsky, S., Ecker, U. K. H., y Cook, J. (2017). Beyond misinformation: Understanding and coping with the “post-truth” era. Journal of Applied Research in Memory and Cognition, 6(4), 353-369. https://doi.org/10.1016/j.jarmac.2017.07.008

López, J. C. (2021, 25 de mayo). Amazon Echo Show 10, análisis: características, precio y especificaciones. Xataka.

https://www.xataka.com/analisis/amazon-echo-show-analisis-caracteristicas-precio-especificaciones

Lustig, C., y Nardi, B. (2015, Enero). Algorithmic authority: The case of Bitcoin. En 2015 48th Hawaii International Conference on System Sciences (pp. 743-752). IEEE. https://doi.org/10.1109/HICSS.2015.91

Maarek, P. J. (2014). Marketing político y comunicación: Un enfoque estratégico. Ariel.

Malwarebytes. (s. f.). What is phishing? https://www.malwarebytes.com/phishing

Martin, K. D., Borah, A., y Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. Journal of Marketing, 81(1), 36-58. https://doi.org/10.1509/jm.15.0497

Martin, K. D., y Murphy, P. E. (2016). The role of data privacy in marketing strategy. Journal of the Academy of Marketing Science, 45(2), 135-155. https://doi.org/10.1007/s11747-016-0495-4

Meyrowitz, J. (1986). No Sense of Place: The Impact of Electronic Media on Social Behavior. Oxford University Press.

Miranda, L. (2023, 15 de noviembre). Amazon lanza una nueva versión de Astro, el robot inteligente. Hipertextual. https://hipertextual.com/2023/11/amazon-lanza-nueva-version-astro-robot-inteligente

Miranda, L. (2023, 15 de noviembre). Amazon lanza una nueva versión de Astro, su robot inteligente. Hipertextual. https://hipertextual.com/2023/11/amazon-lanza-nueva-version-astro-robot-inteligente

Newman, G. R., y Clarke, R. V. (2013). Superhighway robbery: Preventing e-commerce crime. https://doi.org/10.4324/9781843924876

NortonLifeLock. (2021). Informe Norton sobre Seguridad de Datos 2021. NortonLifeLock Inc.

Padilla, G. (2023, 1 de marzo). Google: 8 de cada 10 usuarios investigan en línea antes de comprar. Revista NEO. https://www.noticiasneo.com/index.php/articles/2023/03/01/google-8-de-cada-10-usuarios-investigan-en-linea-antes-de-comprar

Panetta, K. (2018, 15 de octubre). Gartner top 10 strategic technology trends for 2019. Gartner.

https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2019

Pantano, E., y Viassone, M. (2015). Engaging consumers on new integrated multichannel retail settings: Challenges for retailers. Journal of Retailing and Consumer Services, 25, 106-114. https://doi.org/10.1016/j.jretconser.2015.04.003

Pappano, L. (2012). The Year of the MOOC. The New York Times. https://www.nytimes.com/2012/11/04/education/edlife/massive-open-online-courses-are-multiplying-at-a-rapid-pace.html

Pastor, J. (2021, 29 de septiembre). Un lobo con piel de cordero: Astro, el robot de Amazon, es una pesadilla para la privacidad según documentos filtrados. Xataka. https://www.xataka.com/robotica-e-ia/lobo-piel-cordero-astro-robot-amazon-pesadilla-para-privacidad-documentos-filtrados

Peirano, M. (2023, 28 de enero). Google atasca la ley europea de propaganda política online. *El País.* https://elpais.com/opinion/2023-01-28/google-atasca-la-ley-europea-de-propaganda-politica-online.html

Peirano, M. (2023). Google atasca la ley europea de propaganda política "online". *El País*. https://elpais.com

Peirano, M. (2023). Google y propaganda política. *El País*.

Pine, B. J., y Gilmore, J. H. (1999). The Experience Economy: Work is Theatre y Every Business a Stage. Harvard Business Review Press.

PwC. (2021). PwC's Global Consumer Insights Survey 2021: Understanding consumer behaviors and trends in the digital age. PricewaterhouseCoopers. https://www.pwc.com/gx/en/consumer-markets/consumer-insights-survey/2021/gcis-june-2021.pdf

Ring. (2021). Ring: Smart security devices. https://www.ring.com

Rodríguez de Luis, E. (2021, 25 de mayo). Amazon Echo Show 10, análisis: características, precio y especificaciones. Xataka. https://www.xataka.com/analisis/amazon-echo-show-10-analisis-caracteristicas-precio-especificaciones

Rodríguez, J. (2023, 11 de febrero). Superaño electoral: Así ruge la sala de máquinas de la política española. *El País*. https://elpais.com/eps/2023-02-11/superano-electoral-asi-ruge-la-sala-de-maquinas-de-la-politica-espanola.html

Römer, M. (2014). Comunicación en campaña: Dirección de campañas electorales y marketing político. (J. C. Herrero, Ed.). Pearson.

Saleslion. (2024). 81% of consumers conduct online research before making big purchases, study finds. GE Capital Retail Bank. https://www.saleslion.com/study-ge-capital-retail-bank-consumer-research

Sanchís Armelles, J. L. (2014). Elementos básicos de una campaña electoral (Tesis doctoral, Universidad Complutense de Madrid). Dirigida por M. Márquez Padorno. https://produccioncientifica.ucm.es/documentos/5d1df62329995204f76626fc

SmartHome News. (2021). Cómo crear perfiles de Alexa para toda tu familia. SmartHome News. https://www.smarthome.news/es/como/amazon/como-crear-perfiles-de-alexa-para-toda-tu-familia

Solove, D. J. (2004). The digital person: Technology and privacy in the information age. NYU Press.

Solove, D. J. (2006). A taxonomy of privacy. University of Pennsylvania Law Review, 154(3), 477-560. doi:10.2307/40041279

Sundararajan, A. (2017). The Sharing Economy: The End of Employment and the Rise of Crowd-Based Capitalism. MIT Press.

Susser, D., Roessler, B., y Nissenbaum, H. (2019). Online manipulation: Hidden influences in a digital world. Georgetown Law Technology Review, 4(1), 1-45.

Symantec. (2018). Internet Security Threat Report. Recuperado de https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf

Tapscott, D., y Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. Penguin.

Tene, O., y Polonetsky, J. (2013). Big Data for all: Privacy and user control in the age of analytics. Northwestern Journal of Technology and Intellectual Property, 11(5), 239-273.

Tikkinen-Piri, C., Rohunen, A., y Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer Law & Security Review, 34(1), 134-153. https://doi.org/10.1016/j.clsr.2017.05.015

Tong, C., Wong, S. K. S., y Lui, K. P. H. (2012). The influences of service personalization, customer satisfaction, and switching costs on e-loyalty. International Journal of Economics and Finance, 4(3), 105-114. https://doi.org/10.5539/ijef.v4n3p105

Turow, J. (2011). The daily you: How the new advertising industry is defining your identity and your worth. Yale University Press.

van Dijk, J. A. (2006). Digital divide research, achievements and shortcomings. Poetics, 34(4-5), 221-235. https://doi.org/10.1016/j.poetic.2006.05.004

van Dijk, J. A. G. M. (2006). The Network Society: Social Aspects of New Media. Sage Publications.

Verhoef, P. C., Neslin, S. A., y Vroomen, B. (2007). Multichannel customer management: Understanding the research-shopper phenomenon. International Journal of Research in Marketing, 24(2), 129-148. doi:10.1016/j.ijresmar.2006.11.002

Verizon. (2021). 2021 Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/

Voigt, P., y Von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer International Publishing. doi:10.1007/978-3-319-57959-7

Wardle, C., y Derakhshan, H. (2017). Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making. Council of Europe. https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c

Wardle, C., y Derakhshan, H. (2017). Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making. Council of Europe. https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c

Wedel, M., y Kamakura, W. A. (2000). Market segmentation: Conceptual and methodological foundations (2nd ed.). Springer Science y Business Media. https://doi.org/10.1007/978-1-4615-4651-1

Wikipedia. (2023). Amazon Echo. Wikipedia. https://es.wikipedia.org/wiki/Amazon_Echo

Yuan, L., y Powell, S. (2013). MOOCs and open education: Implications for higher education. JISC CETIS. https://publications.cetis.ac.uk/2013/667

Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs.