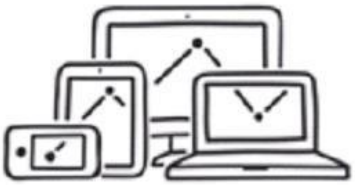
Global Guideline

Mobile Research



ESOMAR
WORLD RESEARCH

GLOBAL RESEARCH
BUSINESS NETWORK
APRC • EFAMRO • ARIA • AMRA

ESOMAR/GRBN GUIDELINE ON MOBILE RESEARCH

ESOMAR es la voz global de la comunidad de los datos, la investigación e insights, en representación de más de 5000 profesionales y más de 500 empresas que proporcionan o comisionan análisis e investigación de datos en más de 130 países, todos los cuales acuerdan respetar el Código Internacional ICC/ESOMAR**.**

GRBN, Global Research Business Network, conecta a 45 asociaciones de investigación y más de 3500 empresas de investigación de los cinco continentes. www.grbn.org.

ÍNDICE

1 INTRODUCCIÓN Y ALCANCE

La presente Guía ESOMAR/GRBN sobre investigación móvil tiene por objeto ayudar a los investigadores, especialmente a los de las pequeñas y medianas organizaciones de investigación, a tener en cuenta consideraciones jurídicas, éticas y prácticas al realizar investigaciones con dispositivos móviles. Explica cómo aplicar los principios fundamentales de mercado, opinión e investigación social en el contexto de los actuales marcos legales y entornos regulatorios en todo el mundo. Sustituye a las directrices anteriores publicadas por ESOMAR y GRBN en 2012 y 2014 respectivamente. Se trata de una declaración de principios globales y no de un catálogo de normativas existentes.

La presente Guía no pretende sustituir la lectura y comprensión exhaustivas del Código Internacional ICC/ESOMAR sobre Investigación de Mercados, Opinión e Investigación Social y Análisis de Datos, ni los códigos individuales de las 45 asociaciones que componen el GRBN. Más bien, pretende servir como una interpretación de los principios fundamentales de esos códigos en el contexto de la investigación donde los individuos comparten datos o información en cualquier entorno o forma que pueda permitir identificar a un individuo.

Por último, esta Guía reconoce que la tecnología y las regulaciones gubernamentales continúan evolucionando, y que puede haber diferentes leyes y regulaciones en diferentes países. Por lo tanto, busca satisfacer tres requisitos clave:

1. Ser coherente con el espíritu y el contenido de las leyes existentes.
2. Reflejar los principios éticos y profesionales de la industria establecidos en nuestros códigos profesionales.
3. Ser lo suficientemente amplia y flexible para abordar las tendencias actuales y futuras previstas en la investigación móvil.

1.1 Alcance

Esta Guía cubre la recopilación y el uso de datos personales mediante dispositivos móviles (teléfonos móviles, tabletas y otros dispositivos informáticos móviles similares) con fines de investigación de mercado, opinión o social y análisis de datos (en lo sucesivo, "investigación"). También reconoce que estos dispositivos permiten muchas otras actividades, como el uso general de Internet, la publicación en redes sociales, el consumo de diferentes tipos de medios y las compras en línea, por nombrar algunas. Estos datos también pueden utilizarse para la investigación.

Describe la responsabilidad de los investigadores cuando trabajan tanto con datos primarios recopilados para fines de investigación como con datos secundarios que pueden haber sido recopilados para algún otro propósito, pero utilizados en la investigación. Describe las prácticas necesarias para cumplir con los códigos, directrices y requisitos legales pertinentes de la industria en las jurisdicciones locales donde se lleva a cabo la investigación.

Esta Guía también reconoce que una amplia gama de terceros puede participar como subcontratistas en la recopilación, preparación, análisis, almacenamiento y entrega de datos. Dichos terceros tienen las mismas obligaciones que los investigadores cuando se trata de datos personales.

Muchas de las prácticas descritas en esta Guía, especialmente las relacionadas con el consentimiento y la protección de la privacidad, son similares a las que se requieren para la investigación en línea. Se recomienda ampliamente a los investigadores que consulten la Guía de Investigación en Línea de ESOMAR/GRBN, la Guía de ESOMAR/GRBN sobre la Calidad de las Muestras en Línea y la Lista de Control de Protección de Datos de ESOMAR donde se describen más detalladamente muchos de los requisitos y/o recomendaciones.

A lo largo de este documento se utiliza la palabra "deberá" para identificar los requisitos obligatorios. Usamos la palabra "deberá" cuando describimos un principio o práctica que los investigadores están obligados a seguir. La palabra "debería" se usa al describir la implementación. Este uso pretende reconocer que los investigadores pueden optar por implementar un principio o práctica de diferentes maneras dependiendo del diseño de su investigación.

2 DEFINICIONES

Para efectos de la presente Guía, los siguientes términos tendrán un significado específico:

Panel de acceso significa una base de datos de posibles encuestados que declaran que cooperarán para una futura recopilación de datos si son seleccionados.

Menores (niños y jóvenes) significa individuos para quienes los padres o adultos responsables deben dar permiso para participar en la investigación. Las definiciones de la edad de un niño varían sustancialmente y se establecen en las leyes nacionales y los códigos de autorregulación. A falta de una definición nacional, se define a un niño como de 12 años o menos, y a un "joven" como de 13 a 17 años.

Cliente significa cualquier persona u organización que solicite, encargue o se suscriba a un proyecto de investigación de mercado**.**

Consentimiento significa la indicación libre e informada del permiso de una persona para la obtención y procesamiento de sus datos personales**.**

Interesado (a quien se refieren los datos) significa cualquier persona cuyos datos personales se utilizan en la investigación.

ID de dispositivo significa un número distintivo asociado a un teléfono móvil o dispositivo móvil similar. Los IDs de dispositivo son independientes de los números de serie del hardware. El término "ID de dispositivo" se utiliza a menudo en la investigación para describir la "toma de huellas digitales".

Divulgación deductiva significa la deducción de la identificación del interesado mediante análisis cruzado, muestras pequeñas o mediante la combinación con otros datos (tales como los registros de un cliente o datos secundarios del dominio público).

Toma de huellas digitales significa un conjunto de datos de configuración sobre el dispositivo de un participante (como una computadora, teléfono móvil o tableta) que se pueden utilizar para crear una huella digital de una máquina o dispositivo. Dichos sistemas asumen que la "huella digital de la máquina" identifica de manera única los ajustes y características del usuario de un dispositivo asociado con un dispositivo individual o, potencialmente, una cuenta de usuario individual**.**

Codificación facial se refiere a un método de codificar los movimientos musculares faciales de un individuo para inferir reacciones emocionales en respuesta a diversos estímulos, como un anuncio publicitario o un nuevo concepto de producto. Esto es distinto del reconocimiento facial, donde el objetivo es identificar a un individuo específico en una imagen digital.

Geolocalización significa la ubicación geográfica de un dispositivo, como una computadora, teléfono móvil, tableta, etc.

GPS (sistema de posicionamiento global) significa cualquier sistema de navegación por satélite que proporciona información sobre la ubicación y la hora sobre todas las condiciones meteorológicas, en cualquier lugar de la tierra o cerca de ella, donde haya una línea de visión sin obstáculos para cuatro o más satélites GPS.

Daño significa daño tangible y material (tales como lesión física o pérdida financiera), daño inmaterial o moral (tales como daño a la reputación o buena voluntad), o intrusión excesiva en la vida privada, incluyendo mensajes de publicidad no solicitados y dirigidos personalmente.

IoT (Internet de las Cosas) significa la red de dispositivos físicos, vehículos, edificios y otros elementos integrados con electrónica, software, sensores, actuadores y conectividad de red que permiten a estos objetos recopilar e intercambiar datos**.**

Dispositivo móvil significa un dispositivo pequeño, ligero y portátil (como un teléfono móvil o tableta) que normalmente tiene una pantalla de visualización con entrada táctil y/o un teclado en miniatura.

Teléfono móvil (también conocido como teléfono celular, teléfono celular y teléfono de mano) significa un dispositivo que puede hacer y recibir llamadas telefónicas a través de un radioenlace mientras se desplaza por una amplia zona geográfica.

Mistery shopping (comprador misterioso) significa el uso de recopiladores de datos capacitados para observar, experimentar y medir un proceso de servicio al cliente actuando como cliente o cliente potencial y realizando una serie de tareas predeterminadas para evaluar el desempeño en comparación con los parámetros de calidad del servicio, o para recopilar información sobre las ofertas de la competencia.

Actividad no relacionada con la investigación significa tomar acción directa hacia un individuo cuyos datos personales fueron recopilados o analizados con la intención de cambiar las actitudes, opiniones o acciones de ese individuo.

Paradatos se refiere a los datos sobre el proceso por el que se recopilaron los datos, e incluye el comportamiento de los interesados durante la recopilación de los mismos.

Recolección pasiva de datos significa la recolección de datos personales mediante la observación, medición o registro de las acciones o el comportamiento de un individuo.

Datos personales (a veces denominados información de identificación personal o IIP) significa cualquier información relativa a una persona física viva (en lo sucesivo, "el interesado") que pueda utilizarse para identificar a una persona, por ejemplo, haciendo referencia a identificadores directos (como un nombre, una ubicación geográfica específica, un número de teléfono, una imagen, un sonido o una grabación de vídeo) o indirectamente haciendo referencia a las características físicas, fisiológicas, mentales, económicas, culturales o sociales de una persona. La identificación del dispositivo y sus huellas digitales también se consideran datos personales en algunas jurisdicciones**.**

Datos primarios significa datos recopilados por un investigador de o sobre un individuo con fines de investigación.

Aviso de privacidad (a veces denominado política de privacidad) significa un resumen publicado de las prácticas de privacidad de una organización que describe la forma en que una organización recopila, utiliza, divulga y gestiona los datos personales de un individuo.

Investigación, que incluye todas las formas de investigación de mercado, opinión e investigación social y análisis de datos, es la recopilación e interpretación sistemática de información sobre individuos y organizaciones. Utiliza los métodos y técnicas estadísticas y analíticas de las ciencias sociales, conductuales y de datos aplicadas para generar percepciones y apoyar la toma de decisiones por parte de los proveedores de bienes y servicios, los gobiernos, las organizaciones sin fines de lucro y el público en general.

Investigador: toda persona u organización que lleve a cabo o actúe como consultor en materia de investigación, incluyendo a las personas que trabajen en las organizaciones clientes y a los subcontratistas empleados.

Datos secundarios son los datos recopilados con otro fin y utilizados posteriormente en la investigación.

Datos sensibles significa cualquier información sobre el origen racial o étnico, la salud o vida sexual, antecedentes penales, opiniones políticas o creencias religiosas o filosóficas de una persona que pueda identificarla. Puede haber información adicional (p. ej., ubicación o información financiera) definida como sensible en diferentes jurisdicciones**.**

SMS (Short Message Service) es un componente de servicio de mensajería de texto de un sistema de comunicación telefónica, web o móvil, que utiliza protocolos de

comunicación normalizados que permiten el intercambio de mensajes de texto cortos entre dispositivos de línea fija o teléfono móvil**.**

Datos de redes sociales significa información (por ejemplo, comentarios o fotos) que los usuarios generan o comparten mientras están activos en las redes sociales.

Por "dispositivos portables" se entiende los dispositivos electrónicos (sensores) que se llevan debajo, con, encima o como parte de prendas de vestir capaces de recopilar e intercambiar datos sin intervención humana**.**

Historial de navegación web significa la lista de páginas web que un usuario ha visitado recientemente - y los datos relacionados, como el título de la página y la hora de visita - que se graba en el software del navegador web durante un período de tiempo determinado.

3 INTERESADOS, RELACIONES Y RESPONSABILIDADES

3.1 Garantizar que no se provoquen daños

Los investigadores deben tomar todas las precauciones razonables para asegurar que los interesados no resulten perjudicados como resultado del uso de sus datos para la investigación. Para ello, deben considerar cuidadosamente los requisitos específicos de la investigación; consultar los requisitos/restricciones legales, regulaciones y costumbres locales; y considerar las implicaciones prácticas que las actividades de investigación puedan tener en los sujetos de estudio. En todos los casos, los investigadores sólo deben preguntar a los interesados qué es aceptable, seguro y justo desde el punto de vista del interesado.

Los investigadores también deben asegurarse de que cualquier software que proporcionen a los interesados se someta a pruebas exhaustivas, cumpla con las protecciones de privacidad acordadas y no interfiera o dañe el dispositivo móvil. Vea la Sección 6 - Prácticas Inaceptables para más detalles.

3.1.1 Seguridad

Al llamar a teléfonos móviles, los investigadores pueden ponerse en contacto con potenciales interesados que están involucrados en una actividad o en un entorno que normalmente no se encuentra en las llamadas de línea fija. Esto podría incluir conducir un vehículo, manejar maquinaria o caminar en un espacio público. El investigador debe confirmar si el individuo se encuentra en una situación donde es legal, seguro y conveniente tomar la llamada. Si el investigador no recibe confirmación, entonces la llamada debe ser terminada dejando abierta la posibilidad de hacer más intentos en otro momento.

Algunos métodos de investigación móvil implican pedir a las personas que actúen como recopiladores de datos yendo a lugares o realizando tareas específicas. En tales casos, los investigadores deben advertirles sobre cualquier situación que pueda ponerlos en peligro, violar la ley o infringir la privacidad de otros. Los ejemplos incluyen advertirles que no deben enviar mensajes de texto o interactuar con su dispositivo móvil mientras conducen o no tomar fotos o grabar en lugares donde está prohibido (por ejemplo, edificios gubernamentales, bancos, escuelas, áreas de seguridad del aeropuerto, espacios privados o áreas donde se colocan avisos prohibiendo el uso de cámaras).

3.1.2 Confidencialidad y datos sensibles

Un investigador puede ponerse en contacto con un interesado potencial que esté involucrado en una actividad o situación en la que otros puedan escuchar la llamada. En este caso, el investigador debe considerar la posibilidad de que se escuche al interesado y de que la información o el comportamiento personal pueda revelarse inadvertidamente o de que se modifiquen las respuestas como resultado de su situación. En su caso, la llamada deberá reprogramarse en otro momento o lugar en el que no se comprometa la confidencialidad.

Los investigadores también deben tener cuidado al abordar a los interesados con temas delicados debido al riesgo de daño o angustia. En algunos países, puede ser necesaria la autorización de la autoridad nacional competente para recopilar datos sensibles.

3.1.3 Costos

A diferencia de la mayoría de los otros métodos de investigación, los interesados pueden incurrir en costos como consecuencia de participar en la investigación móvil que puede incluir cargos por descargas de datos, acceso en línea, mensajería de texto, excederse en los planes de datos, cargos por roaming, recuperación de mensajes de voz y cargos telefónicos estándar. Los investigadores deben diseñar su investigación de manera que los interesados no incurran en costos sin una aprobación expresa. Si esto no es posible, los investigadores deben estar preparados para ofrecer compensación. Estas compensaciones pueden consistir en efectivo, dinero móvil, tiempo aire u otras formas de valor.

3.1.4 Distinción entre actividades relacionadas y no relacionadas a la investigación

Los investigadores deben asegurarse de que los fines de la investigación se distinguen claramente de las actividades no relacionadas con la investigación. Además, no deberán permitir que los datos personales recabados con fines de investigación se utilicen para cualquier otro propósito sin el consentimiento previo del interesado. Este requisito no impide que los investigadores participen en actividades no relacionadas con la investigación, siempre que, al recopilar datos personales para fines distintos de la investigación, dichos fines se comuniquen expresamente a los interesados, se diferencien razonablemente de cualquier actividad de investigación en la que participen y se obtenga el consentimiento para el uso de los datos con fines distintos de la investigación antes de la recopilación de datos.

3.2 Menores y otros individuos vulnerables

Al realizar investigaciones con niños u otras personas vulnerables, los investigadores deben consultar las leyes nacionales y los códigos de autorregulación en las jurisdicciones donde se recopilarán los datos para determinar cuándo se requiere el permiso de los padres o las sensibilidades culturales requieren un tratamiento particular. Si al ponerse en contacto por teléfono con posibles interesados se hace evidente que el interesado es un niño, el investigador no debe seguir adelante con la entrevista a menos que obtenga permiso de un padre o adulto responsable para invitar al niño a participar en la investigación. Si el individuo no es competente, algunas jurisdicciones pueden exigir que el investigador ofrezca la oportunidad de participar en la investigación utilizando otro método.

Los investigadores deben tener especial cuidado al fotografiar o grabar a niños. Si no se puede obtener permiso, las imágenes de los niños deben ser pixeladas o borradas.

La mayoría de los sistemas operativos móviles tienen características que permiten, si están habilitados, solicitar el consentimiento de los padres antes de instalar una aplicación. Los investigadores deben utilizar estas configuraciones al desarrollar o poner en marcha el desarrollo de una aplicación que se utilice para fines de investigación.

3.3 Notificación, honestidad, consentimiento y naturaleza voluntaria de la investigación

Los investigadores deben obtener el consentimiento de los interesados antes de recopilar cualquier tipo de datos personales y ser completamente transparentes sobre:

- su identidad;
- la información que planean recopilar;
- la finalidad general para la que se recopilará;
- el método de recopilación de datos;
- cuánto tiempo se espera que participe el interesado;
- cómo se protegerán los datos; y

- con quiénes podrían compartirse los datos y en qué forma

Esta información debe ser clara, concisa y prominente. Consulte también la sección 3.7.1 Avisos de privacidad. Además, en caso de que se produzca algún cambio en la información anterior, será necesario el consentimiento de los interesados. Los interesados nunca deben ser manipulados, engañados, no se les mentirá ni forzará.
La participación en la investigación es siempre voluntaria y los interesados deben poder retirar y hacer que sus datos personales sean eliminados en cualquier momento.

Finalmente, los investigadores deben cumplir con todas las leyes, regulaciones y reglas locales de conducta profesional relevantes.

3.3.1 Minimización de datos y carga razonable

Los investigadores deberán limitar la recopilación y/o el manejo de los datos personales a aquellos temas que sean relevantes para la investigación. También deberían garantizar que cualquier tarea asignada a un interesado (por ejemplo, una encuesta, un diario o un foro de discusión) se presente en un formato adecuado para un dispositivo móvil y con una longitud adecuada.

El reducido tamaño de pantalla en algunos dispositivos móviles significa que se debe tener especial cuidado para garantizar que las instrucciones, preguntas o formularios sean claros, legibles y concisos. Esto incluye optimizar el formato de los dispositivos y excluir dispositivos específicos si la encuesta es demasiado larga o compleja para ese dispositivo. Estas prácticas se denominan a menudo con términos como "primero móvil", "agnóstico" y "responsividad".

Mientras que la investigación continúa evolucionando, la evidencia actual sugiere que los interesados móviles esperan interacciones más cortas con los investigadores que en otros modos como encuestas telefónicas o focus groups presenciales.

Se aplican precauciones similares cuando se diseñan encuestas para ser realizadas por un entrevistador mediante teléfono móvil, donde la investigación ha mostrado que es más difícil mantener a los interesados en línea que con teléfonos fijos.

3.3.2 Contactar a sujetos potenciales de datos

La tecnología y las comunicaciones móviles han crecido rápidamente y los marcos jurídicos siguen evolucionando. Estas reglamentaciones afectan indirectamente a un investigador, y podrían interpretarse como que establecen una responsabilidad legal para éste cuando se pone en contacto con un posible interesado a través de un dispositivo móvil, ya sea por teléfono, correo electrónico o mensajes de texto. Por ejemplo, en algunos países, el uso de sistemas automatizados para enviar mensajes de texto está prohibido a menos que se obtenga un consentimiento explícito.

Los investigadores no deben utilizar ningún método subterfugio para obtener direcciones de correo electrónico o números de teléfono móvil de los posibles interesados. Esto incluye el uso de sitios web públicos, el uso de tecnologías o técnicas sin que las personas estén conscientes de ello o la recopilación de datos personales bajo la apariencia de alguna otra actividad que no sea la investigación. Por último, las llamadas a números móviles deben configurarse de manera que muestren el número de la persona que llama. Esta función no debe suprimirse deliberadamente.

Los investigadores deben verificar con el proveedor de la muestra (ya sea un proveedor de muestras o un cliente) que las muestras sólo contengan individuos que tengan expectativas razonables de recibir correo electrónico o mensajes de texto solicitando su participación en la investigación.[1]

Se puede encontrar una discusión completa de las prácticas aceptables en la Sección 3.5 de la Guía de Investigación en Línea de ESOMAR/GRBN.

3.3.3 Investigación telefónica

Al llamar a teléfonos móviles, los investigadores deben reconocer que incluso cuando la legislación restringe las llamadas no solicitadas con fines comerciales, pero no de investigación, es vital consultar y aplicar cualquier lista específica de "no contactar" para

teléfonos móviles y fijos.
Algunos países también tienen leyes o normas que especifican las horas de llamada permitidas para llamadas no solicitadas de cualquier tipo y éstas deben ser respetadas para encuestas a través de teléfonos móviles.
Los investigadores deben anticipar que la persona contactada podría estar en una zona horaria diferente, y por lo tanto verificar la conveniencia de la hora, ubicación y situación. En ausencia de dichos requisitos, los investigadores deben atenerse a las mismas horas de llamada que para la investigación telefónica de línea fija. Para la investigación en el sector de empresa a empresa, los horarios aceptables están implícitos en los horarios de oficina de la empresa en cuestión. Deberá prestarse una atención similar al envío de mensajes de texto a móviles para evitar que el participante reciba la alerta fuera de "horario normal".

Algunos países restringen el uso de marcadores automáticos y otros equipos de marcación automática, incluyendo marcadores predictivos. Otros permiten el uso de dicho equipo sólo si el interesado ha dado su consentimiento expreso previo (por ejemplo, como miembro de un panel de acceso) para que se marque con un equipo de marcación automática. En los casos en que se permiten y utilizan marcadores automáticos, no se permiten las llamadas abandonadas o silenciosas, en los que no existe disponibilidad inmediata de un entrevistador en vivo.

3.3.4 Incentivos

Cuando se ofrezcan incentivos para fomentar la participación en la investigación móvil, los investigadores deberán asegurarse de que los interesados estén claramente informados sobre:

- cuáles serán los incentivos;
- quién los proporcionará;
- cuándo las recibirán los interesados; y
- si se imponen condiciones (por ejemplo, la realización de una tarea específica, el acceso a datos de investigación pasivos, la aprobación de controles de calidad, el tiempo mínimo requerido como miembro activo de una comunidad, etc.).

Los investigadores deben considerar cuidadosamente el uso de incentivos proporcionados por los clientes (tales como productos del cliente o artículos con logotipos de los clientes) ya que estos pueden ser considerados como marketing en algunas jurisdicciones.

Para un análisis completo de los incentivos, incluyendo el uso de concursos y sorteos de premios gratuitos, ver la Sección 3.6 de la Guía de Investigación en Línea ESOMAR/GRBN.

3.4 Recopilación pasiva de datos

Las aplicaciones móviles son capaces de recopilar una amplia gama de datos personales sin interacción directa con los interesados. Algunos ejemplos incluyen el uso de la web y el historial de navegación, estadísticas de uso de aplicaciones, datos de tarjetas de lealtad. geolocalización, datos de redes sociales, datos de dispositivos portables, IoT y otros datos generados u obtenidos desde dispositivos móviles.[2]

Además, tecnologías específicas como el rastreo en línea tienen aplicación válida en la investigación como una forma de recolección pasiva de datos que normalmente incluye:

- mejorar la integridad de las muestras en línea;
- prevención del fraude; o
- aplicaciones de investigación, incluyendo, entre otras, mediciones de audiencia en línea, mediciones de contenido y pruebas publicitarias.

[1] Otras tecnologías de mensajería como las notificaciones de aplicaciones móviles pueden tener características y capacidades similares a los mensajes de texto.

Bajo estas y otras circunstancias similares, los investigadores deben hacer todos los esfuerzos razonables para obtener el consentimiento, tal como se describe en la Sección 3.3. Cuando no sea posible obtener el consentimiento (por ejemplo, al medir el tráfico de un sitio web), los investigadores deben tener motivos legalmente permitidos para recopilar los datos y deben eliminar u ocultar las características de identificación tan pronto como sea posible por razones operativas (vea la Sección 3.7.2 Desidentificación de los datos).

3.4.1 Datos biométricos

La recopilación de datos pasivos y conductuales también puede implicar interacciones directas con los interesados. Por ejemplo, la codificación facial implica registrar la cara del interesado a medida que éste realiza una encuesta o una tarea similar. El rastreo de ojos, los audífonos de realidad virtual y otros dispositivos que se puedan portar pueden usarse de manera similar. Todo esto puede implicar la recopilación de datos personales y, en algunos casos, datos que pueden clasificarse como confidenciales en algunas jurisdicciones que requieren procesos para verificar el cumplimiento de las leyes locales y códigos industriales aplicables.

3.4.2 Fotografías y grabaciones

Las fotografías, grabaciones de vídeo y audio se consideran datos personales y, por lo tanto, deben recopilarse, procesarse y almacenarse como tales. Sólo podrán ser compartidos con un cliente si el interesado otorga su consentimiento previo, con conocimiento de la finalidad específica para la que serán utilizados. Cuando se haya eliminado información potencialmente identificable (por ejemplo, mediante la tecnología de pixelización o modificación de voz) de modo que ya no se considere como datos personales, podrá ser compartida con un cliente siempre que éste acepte no intentar identificar a la persona.

Los investigadores no deben indicar a los interesados (o a quienes puedan estar actuando como recopiladores de datos) que participen en la vigilancia de individuos o lugares públicos. A los interesados se les deben asignar tareas específicas y limitadas (por ejemplo, la captura de interacciones con amigos con su consentimiento, o imágenes de objetos o pantallas) que no impliquen el monitoreo de un área en particular donde los datos personales serían capturados sin el consentimiento de las personas presentes. Cuando se lleve a cabo la observación grabada de un lugar, se colocarán señales claras y legibles que indiquen que el área está bajo observación, junto con los datos de contacto del investigador u organismo de investigación que realiza la investigación, y las imágenes de los individuos deberán ser pixeladas o eliminadas lo antes posible. Las cámaras deben estar situadas de manera que sólo controlen las zonas destinadas a la observación.

[2] Si bien es posible detectar de forma pasiva el tipo de dispositivo que está utilizando un interesado, no se trata de datos personales, siempre que el objetivo sea optimizar el rendimiento de la aplicación y la prestación de la encuesta.

3.4.3 Rastreo en tiendas

El rastreo en tienda de los interesados es una forma de recolección pasiva de datos donde el movimiento de los individuos a través de una tienda se registra mientras compran. Las aplicaciones específicas se clasifican en dos grandes categorías.

En la primera categoría se pide a los interesados que lleven un dispositivo o descarguen una aplicación que se sincronice con hardware (como un faro) para rastrear y registrar el movimiento a través de la tienda. Con este enfoque se aplican los requisitos estándar de notificación y consentimiento (vea la Sección 3.3 - Notificación, honestidad, consentimiento y naturaleza voluntaria de la investigación).

En la segunda categoría, es posible que a los interesados no se les haya dicho explícitamente que están siendo observados y que se están recopilando datos de comportamiento mientras están en la tienda. En tales casos, los investigadores deben asegurarse de que:

- el monitoreo y la recopilación de datos está permitido por la ley local;
- hay señales claras que indican que se está registrando el comportamiento; y
- todas las características de identificación se eliminan u ocultan lo antes posible por razones operativas.

3.5 Mystery shopping

Los interesados (generalmente empleados) en estudios de compradores misteriosos (mystery shopping) generalmente no están conscientes de que están siendo observados. Los investigadores deben cuidar que se respete la intimidad individual y de que los interesados no se vean perjudicados o afectados de ningún modo por el hecho de ser objeto de un ejercicio de mystery shopping. Sus datos personales deben ser protegidos y no se pueden compartir fotografías o grabaciones con el cliente a menos que se haya obtenido el permiso de los interesados, generalmente como parte de un contrato de trabajo.

Mystery shopping se distingue de la recopilación de datos en el momento, diseñada para capturar la reacción del interesado a las características de la experiencia de compra y su influencia en las decisiones de compra, que es una forma de etnografía realizada con consentimiento.

3.6 Uso de datos secundarios

En esta era digital se crea una cantidad cada vez mayor de datos como producto incidental de las transacciones y actividades diarias. Por ejemplo, los proveedores de servicios móviles a menudo recopilan gran cantidad de información sobre sus clientes y su uso de dispositivos móviles. Los teléfonos móviles crean registros no sólo de quiénes son los usuarios que llaman y quiénes los llaman, sino también datos de geolocalización de dónde han estado, sitios web que han visitado, con qué torres de telefonía móvil se han conectado, etcétera. También pueden registrar información sobre el uso de aplicaciones individuales e incluso datos como publicaciones en redes sociales.

Estos y otros datos similares presentan nuevas oportunidades para que los investigadores amplíen su comprensión del comportamiento de las personas. Si bien los investigadores a veces diseñan proyectos para recopilar algunos de estos tipos de datos utilizando métodos tradicionales, es posible que gran parte de ellos ya existan como datos secundarios que pueden estar disponibles para su reutilización.

Antes de utilizar estos datos, los investigadores deben asegurarse de que:

- su uso previsto está permitido legalmente en los términos acordados con los interesados antes de la obtención de datos y no está específicamente excluido en el aviso de privacidad proporcionado en el momento de la obtención original;
- los datos no fueron recabados en violación de las restricciones impuestas por la ley, mediante engaño o de maneras que no fueran aparentes o razonablemente discernibles y anticipadas por el interesado;
- Los interesados tengan una expectativa razonable de que los datos puedan ser utilizados para algún otro propósito, como investigación;
- se cumpla cualquier petición de los interesados de que sus datos no se utilicen para otros fines; y
- la organización que proporciona los datos debe tener el derecho legal de compartirlos.

Los investigadores también deben considerar si el procesamiento posterior de los datos podría causar daño a los interesados a través de la divulgación deductiva. Si existen tales riesgos, los investigadores deben establecer salvaguardias para mitigar el riesgo de tales daños. Esto incluye, entre otras cosas, la garantía de que no se divulgue o revele la identidad de los interesados sin su consentimiento previo y que no se les dirija ninguna actividad no relacionada con la investigación como consecuencia directa de que sus datos se hayan utilizado para la investigación.

3.7 Protección de datos y privacidad

Los investigadores deben adherirse a los principios universales de protección de datos[3] para los datos personales. Estos principios establecen que los datos personales

obtenidos o utilizados deben ser:

- obtenidos para un fin determinado y no utilizados de manera incompatible con dicho fin;
- adecuados, pertinentes y no excesivos en relación con la finalidad para la que se obtuvieron y/o trataron posteriormente;
- no se hayan obtenido en violación de las restricciones impuestas por la ley, mediante engaño o de maneras que no fueran aparentes o razonablemente discernibles y anticipadas por el interesado;
- no se utilicen de forma que pueda perjudicar a los interesados, incluida la adopción de medidas para protegerse de tales daños;
- protegidos contra riesgos tales como pérdida, acceso no autorizado, destrucción, uso, manipulación o divulgación; y
- conservados por un período no superior al necesario para la finalidad para la que se recopiló o trató la información.

Existen diversas normas y marcos que los investigadores deben utilizar para elaborar las normas y políticas de seguridad de datos necesarias. Para más información, los investigadores pueden consultar la norma ISO 27001: Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Requisitos o Lista de comprobación de ESOMAR para la protección de datos.

Los investigadores deben considerar cuidadosamente cualquier decisión de almacenar datos personales en la nube. Deben evaluar los controles de seguridad del proveedor de servicios de almacenamiento en la nube y sus términos y condiciones estándar, y estar preparados para implementar controles compensatorios cuando los controles del proveedor no sean suficientes. Para más detalles, consulte la Sección 7.7 de la Guía de investigación en línea de ESOMAR/GRBN, la Lista de comprobación de protección de datos de ESOMAR y la Guía práctica para el computo en nube.

[3] Ver por ejemplo los Principios de Privacidad de la OCDE.

3.7.1 Avisos de Privacidad

Las leyes y regulaciones de privacidad generalmente requieren que las compañías de investigación proporcionen un aviso de privacidad a los interesados. Debido a las limitaciones del tamaño de la pantalla de los dispositivos móviles, los investigadores deberían considerar el uso de avisos de privacidad en capas. Por lo general, se trata de un aviso breve que contiene información básica, como la identidad de la organización y la forma en que se utilizarán los datos personales, además de un aviso más extenso.

Los interesados deben contar con información suficiente basada únicamente en un breve aviso previo para indicar su consentimiento y se debe destacar las prácticas y usos de los datos que puedan no ser obvios, como el sonido y las imágenes, la ubicación geográfica, el uso secundario, el intercambio y la retención de datos, en lugar de los tipos obvios de datos recopilados, como el nombre, la edad y las opiniones.

El aviso breve debe contener un enlace a una segunda descripción más detallada y toda la información debe ser fácilmente visible sin tener que desplazarse por las pantallas diseñadas para ser vistas desde un equipo de escritorio.

El aviso de privacidad debe indicar bajo qué ley (es) se recopilan los datos. Si se recolectan datos en varios países, el investigador debe cumplir con las leyes de los países donde se lleva a cabo la investigación. Cuando sea posible conocer el país de residencia de los interesados, los investigadores deben seguir los requisitos legales de ese país, considerando que puede haber una variación considerable entre las distintas jurisdicciones.

3.7.2 Desidentificación de los datos

Los investigadores deben asegurarse de que los datos compartidos con clientes u otros usuarios de datos estén lo suficientemente desidentificados como para evitar la divulgación de datos personales. Existe una gran variedad de técnicas de desidentificación, cada una de las cuales proporciona diferentes niveles de protección contra la divulgación de datos personales y/o medidas de seguridad adicionales. Cubren una amplia gama de manipulaciones de datos que incluyen la eliminación de identificadores directos, la eliminación de identificadores indirectos (elementos potencialmente sujetos a divulgación deductiva) y transformaciones de datos (por ejemplo, hashing, cifrado, agregación).

La seudonimización es una técnica especialmente popular para desidentificar los datos durante el procesamiento y cuando puede ser necesario volver a crear los datos originales para fines como la comparación o la validación. Generalmente implica la separación de los datos personales de los datos de investigación, llevar diferentes IDs en cada archivo y crear un tercer archivo que vincule los dos IDs en caso de ser necesario. El acceso al archivo de enlace está limitado a unas pocas personas. Se recomienda ampliamente a los investigadores seudonimizar los datos lo antes posible después de la adquisición.

La anonimización implica una variedad de técnicas en las que los datos personales se eliminan o modifican, de modo que ya no es posible volver a identificar a las personas afectadas, ni siquiera mediante la divulgación deductiva. Entre los ejemplos se incluyen la eliminación o el cifrado de elementos de datos individuales, imágenes borrosas para ocultar caras en fotografías y vídeos, la introducción de ruido y la presentación de resultados como estadísticas agregadas.

3.7.3 Seguridad del dispositivo

Los datos personales almacenados localmente en el dispositivo móvil de un interesado pueden estar disponibles para otras personas en caso de que el dispositivo sea robado o utilizado por otra persona. Los ejemplos incluyen datos almacenados en aplicaciones de recolección de datos de investigación o no relacionados con la investigación instaladas en el dispositivo; fotografías tomadas durante actividades etnográficas u otras actividades de investigación en el contexto; y SMS, correo electrónico u otro tipo de mensajes que puedan haberse utilizado para transmitir datos de investigación que incluyan datos personales.

Cuando se recolectan datos de artículos portables y otros dispositivos IoT, los investigadores deben asegurarse de que todos los datos estén encriptados antes de ser transferidos entre dispositivos.

Los interesados deben estar conscientes de estos riesgos y los investigadores deben aplicar prácticas para proteger los datos personales. Ejemplos de ello son el cifrado de datos (incluida la codificación de datos en reposo y los datos en tránsito), la protección mediante contraseña del dispositivo, e indicar a los interesados cómo borrar toda la información personal al finalizar la investigación u otras medidas de seguridad o control.

3.7.4 Uso de IDs estáticos y dinámicos

Los clientes de la investigación y los proveedores de muestras a veces utilizan identificadores estáticos del interesado (IDs estáticos) para ayudar en el control y la asignación de los interesados, tanto en estudios ad hoc como longitudinales. Esta técnica ha ayudado a consolidar la información sobre cada interesado y se ha convertido en un método útil para garantizar que los interesados sean únicos dentro de un único estudio longitudinal y/o la adherencia a los períodos de exclusión del estudio de investigación.

Comentado [JV1]: IDs estáticos

Algunos proveedores de muestras prefieren identificadores dinámicos (ID variables para cada uso) para salvaguardar la identidad de los distintos interesados.

Comentado [JV2]: ID Variables para cada uso

Los investigadores deben considerar cuidadosamente el uso de cada tipo de identificador, equilibrando la privacidad del interesado y las consideraciones de calidad de la investigación en el contexto de su estudio específico.

3.7.5 Uso y controles de los paradatos

Los investigadores sólo deben utilizar los paradatos cuando exista un acuerdo legal mutuo entre el proveedor de la muestra y el cliente para guiar, limitar y proteger la recolección,

uso y posterior transferencia de estos datos sobre el proceso de recolección de datos en el proceso de investigación y análisis subsiguiente. En algunas jurisdicciones se considera que los paradatos son datos confidenciales.

3.7.6 Transferencia transfronteriza

Antes de transferir datos personales del país de obtención a otro país, el investigador debe asegurarse de que la transferencia de datos sea legal y que se tomen todas las medidas razonables para garantizar la privacidad y seguridad de estos datos. Esto se aplica si un servidor de recopilación de datos se encuentra en un país distinto al del interesado. También se aplicará si la tecnología de nube se utiliza para el almacenamiento de datos ubicados en otro país.

El investigador debe comprender las leyes y reglamentaciones de privacidad aplicables de los países de origen y destino que rigen dichas transferencias transfronterizas, señalando que pueden existir mecanismos alternativos para facilitar la transferencia de datos.

3.7.7 Notificación de violación

Los investigadores deben cumplir con todas las leyes y regulaciones relevantes con respecto a la notificación de violación y los requisitos de protocolo para el país donde se están recolectando los datos. Los investigadores deben informar a la autoridad competente en primer lugar de las infracciones de seguridad o de datos, si las hubiere, y luego a todas las partes afectadas, incluidos los clientes, los interesados y los subcontratistas, sin retrasos injustificados. La notificación debe incluir una descripción de los tipos de datos que participaron en la violación y de las medidas que los interesados deben tomar para protegerse del daño potencial resultante de la violación.

3.8 Compartir datos personales con un cliente

A menos que las leyes y/o regulaciones de privacidad aplicables estipulen un requisito más alto, si los investigadores planean recopilar datos personales para investigación que también puedan ser utilizados para un propósito no relacionado con la investigación, esto debe ser aclarado a los interesados antes de la recopilación de datos y su consentimiento para los fines no relacionados con la investigación.

Los investigadores no deben compartir la información personal identificable del interesado con un cliente a menos que el interesado haya dado su consentimiento y haya aceptado el propósito específico para el que se utilizará.

Incluso cuando se proporcionan a los clientes conjuntos de datos anónimos, los investigadores deben obtener del cliente una garantía por escrito de que no se intentará volver a identificar a los interesados a menos que se cumplan las condiciones anteriores.

3.8.1 Observadores

Algunas formas de investigación incluyen individuos que pueden tener acceso a los datos personales en virtud de la observación de la recopilación de datos en tiempo real o en algún momento posterior a través de vídeo o un panel de control del cliente. Algunos ejemplos incluyen a miembros del equipo de clientes que no son investigadores o subcontratistas de clientes, como las agencias de publicidad. En tales casos, los investigadores deberán obtener:

- el consentimiento de los interesados para ser respetados por dichas personas (incluyendo sus afiliaciones) durante o después de la recopilación de datos; y
- el compromiso formal de todos los clientes y otros observadores de abstenerse de revelar los datos personales del interesado o de utilizarlos de cualquier otra manera que no sea para fines de investigación sin su consentimiento.

4 CLIENTES: RELACIONES Y RESPONSABILIDADES

4.1 Subcontratación

Los investigadores deben informar a los clientes, antes de comenzar el trabajo, cuando cualquier parte del trabajo deba subcontratarse fuera de la propia organización del investigador. Si el cliente lo solicita, debe ser informado de la identidad de dicho subcontratista.

En los casos en que la identidad de un subcontratista a quien se recurra para la obtención de muestras pueda considerarse de forma legítima información protegida, el proveedor de la muestra deberá proporcionar:

- una descripción del tipo de fuentes de la muestra que se utilizará; y
- una estimación del porcentaje de la muestra que se espera obtener de fuentes de panel y fuentes distintas a los paneles.

También se requiere que los investigadores se aseguren de que cualquier dato personal compartido con un subcontratista se limite a lo que se requiera para realizar las tareas de subcontratación; que el subcontratista cuente con los procedimientos de seguridad de datos necesarios para proteger los mismos; y que las responsabilidades del subcontratista en materia de protección de datos estén claramente documentadas y aceptadas.

4.2 Calidad metodológica

Para que los usuarios de la investigación móvil confíen en que los datos obtenidos son adecuados para el fin que pretenden, los investigadores deben poner a disposición de los clientes información adecuada sobre la forma en que se llevó a cabo la investigación, que les permita evaluar la validez de los resultados, incluidas las limitaciones de la metodología que podrían llevar a conclusiones no respaldadas por los datos. Esta información debe incluir:

- tamaño, fuente y gestión de la muestra;
- diseño y selección de muestras;
- el método de recopilación de datos;
- cualquier tipo de limpieza de datos, ponderación o ajustes posteriores al campo que se hayan aplicado; y
- si la penetración móvil es inferior al 100 %, medidas adoptadas para garantizar que los resultados de la investigación representen la población objetivo del estudio

Los requisitos específicos para cada una de estas áreas se pueden encontrar en la Guía ESOMAR/GRBN sobre la calidad de las muestras en línea y en la sección 6 de la Guía de investigación en línea de ESOMAR/GRBN.

4.3 Transparencia, falsa declaración y corrección de errores

Todos los proyectos de investigación deben ser informados y documentados con precisión, transparencia y objetividad. En el caso de que se descubran errores después de la entrega, el cliente debe ser notificado inmediatamente y las correcciones deberán realizarse rápidamente.

5 EL PÚBLICO EN GENERAL: RELACIONES Y RESPONSABILIDADES

5.1 Mantener la confianza del público

Los investigadores deben ser honestos, veraces y objetivos y velar por que su investigación se lleve a cabo de conformidad con los principios, métodos y técnicas pertinentes de investigación científica. Los investigadores siempre deben comportarse de manera ética y no deben hacer nada que pueda dañar la reputación de la investigación de mercado, opinión y social y análisis de datos. Deben tener siempre presentes los principios básicos de los códigos ICC/ESOMAR y GRBN en su labor, evitando actividades y prácticas que puedan socavar la confianza pública.

5.2 Publicación de resultados

Vea la Sección 5.2 de la Guía de Investigación en Línea de ESOMAR/GRBN si desea un

análisis de las responsabilidades del investigador cuando el cliente pretende publicar los resultados de la investigación.

6 PRÁCTICAS INACEPTABLES

Los investigadores no deben utilizar o instalar software o aplicaciones que:

- no se han sometido a pruebas exhaustivas;
- modifican los entornos móviles más allá de lo necesario para llevar a cabo la investigación, sin el consentimiento del interesado;
- ocasionan conflictos con el sistema operativo o provocan que otro software instalado se comporte de manera irregular o inesperada;
- están ocultos dentro de otro software que se puede descargar o que es difícil de desinstalar;
- entregan contenido publicitario, a excepción de lo que pueda ser necesario para la investigación publicitaria legítima;
- alteran los datos recabados sin notificar al interesado y ofrecen la posibilidad de optar por no hacerlo;
- causan una demanda inusualmente alta en la batería del dispositivo a menos que se obtenga un consentimiento específico;
- ocasionan a la persona interesada costos sin consentimiento y que no son reembolsados por el investigador;
- utilizan software de geolocalización sin el consentimiento del interesado;
- transmiten datos personales que no están encriptados;
- alteran la naturaleza de cualquier tecnología de identificación y seguimiento sin notificar y obtener el consentimiento del interesado;
- no notifican al interesado los cambios en la política de privacidad relativos a una actualización;
- recopilan datos personales que pueden ser utilizados por el proveedor de aplicaciones para fines ajenos a la investigación sin consentimiento; o
- extraen información del dispositivo móvil o teléfono móvil a menos que dicha información forme parte de la finalidad del estudio y se obtenga su consentimiento.

Una vez finalizada la investigación, cualquier aplicación que ya no sea necesaria debe ser desactivada. Se notificará a los interesados y se les proporcionarán instrucciones sobre cómo retirar la aplicación de sus dispositivos de forma segura.

7 EQUIPO DEL PROYECTO

- Reg Baker, copresidente de ESOMAR, Director Ejecutivo, MRII y consultor de PSC, EE. UU.
- Guy Rolfe, copresidente de GRBN, Líder de Práctica Móvil, Innovación y Nuevas Tecnologías, Kantar, Reino Unido.
- Mario Callegaro, investigador científico senior de encuestas, Google, Reino Unido
- Simon van Duivenvoorde, Director Comercial, Wakoopa, NL
- Steve Gutterman, CEO de Mobile Accord, Inc.
- Betsy Leichliter, Leichliter Associates, LLC, EE. UU.
- Oriol Llaurado, Director General de Privacidad, Netquest, España
- Peter Milla, Consultor de la Asociación de Insights, EE. UU.
- Paul Quinn, Director Senior, Gestión de Productos, Confirmit, Reino Unido
- Lisa Salas, Directora de Marketing y Operaciones, TEG Rewards, Australia
- Michael Schlueter, Director Asociado de Innovación Global, GfK, Reino Unido

- Navin Williams, CEO, Mobile Measure, Singapur

ESOMAR: Kathy Joe, Directora de Estándares Internacionales y Asuntos Gubernamentales y Jan Willem Knibbe, Ejecutivo de Proyectos de Políticas e Industria.

8 TRADUCCIÓN AL ESPAÑOL

AMAI Comité de Promoción de la Calidad
Revisión: Jorge A. Valdés G., Director General de Evamerc