Guía Global

Investigación mediante dispositivos móviles

ESOMAR
WORLD RESEARCH

GLOBAL RESEARCH
BUSINESS NETWORK
APRO • EFAMRO • ARIA • AMPA

ESOMAR es el portavoz mundial de la comunidad de datos, investigación y análisis, representando a más de 500 profesionales individuales y 500 empresas que prestan o encargan análisis de datos o investigación en más de 130 países, aceptando todos ellos el Código Internacional CCI/ESOMAR**.**

GRBN, el Global Research Business Network, engloba a 45 asociaciones de investigación y a más de 3.500 empresas de investigación en los cinco continentes. www.grbn.org

ÍNDICE

1 INTRODUCCIÓN Y ALCANCE

Esta Guía ESOMAR/GRBN sobre Investigación Mediante Dispositivos Móviles pretende ayudar a los investigadores, especialmente a aquéllos en pequeñas o medianas organizaciones, a afrontar las consideraciones legales, éticas y prácticas cuando realicen una investigación usando dispositivos móviles. Esta Guía explica cómo aplicar los principios fundamentales de la investigación de mercado, social y de la opinión en el contexto de la estructura legal vigente en el mundo. Esta Guía sustituye otras guías separadas emitidas por ESOMAR y GRBN en 2012 y 2014 respectivamente. La Guía contiene una declaración de principios globales más que un catálogo de la normativa existente.

Esta Guía no pretende sustituir la lectura y comprensión en profundidad del Código Internacional CCI/ESOMAR sobre Investigación de Mercado, Social, de la Opinión y del Análisis de Datos, o los códigos individuales de las 45 asociaciones que componen el GRBN. Más bien se trata de una interpretación de los principios fundacionales de dichos códigos en el contexto de una investigación en la que los individuos comparten datos o información de cualquier forma o situación que permita identificar a un individuo.

Finalmente, esta Guía reconoce que la tecnología y las disposiciones gubernativas están en continua evolución, y que pueden existir diferencias en la legislación de los distintos países. Por tanto, pretende satisfacer tres requisitos básicos:

1. Ser consistente tanto con la letra como con el espíritu de la legislación existente.
2. Reflejar los principios éticos y profesionales del sector, tal y como están definidos en nuestros códigos profesionales.
3. Ser suficientemente amplio y flexible para atender tanto la investigación actual mediante dispositivos móviles, como las posibles tendencias futuras.

1.1 Alcance

Esta Guía abarca la recogida y uso de datos personales mediante dispositivos móviles (teléfonos móviles, tabletas y otros dispositivos móviles similares) con fines de investigación de mercado, social o de la opinión y para el análisis de datos (denominado en adelante como “investigación”). También reconoce que estos dispositivos permiten muchas otras actividades, incluyendo el uso general de Internet, la interacción en redes sociales, el consumo de diferentes tipos de medios y las compras online, sólo por mencionar algunos. Estos datos también pueden ser empleados en la investigación.

Esta Guía describe la responsabilidad de los investigadores, tanto cuando trabajan con datos primarios recogidos con fines de investigación, como con datos secundarios que puedan haber sido recogidos para otras finalidades pero que se utilizan en una investigación. Esta Guía describe las practicas necesarias para cumplir con los códigos sectoriales relevantes, con las guías y con los requisitos legales aplicables en aquellas jurisdicciones donde se desarrolle la investigación.

Esta Guía reconoce que pueden participar una amplia gama de terceros (por ejemplo, subcontratistas) en la recogida, preparación, análisis, conservación y entrega de datos. Estos terceros tienen las mismas obligaciones que los investigadores en lo relativo a los datos personales.

Muchas de las practicas descritas en esta Guía -especialmente aquéllas relacionadas con el consentimiento y la protección de la privacidad- son similares a las requeridas para la investigación online. Se recomienda encarecidamente a los investigadores que consulten la Guía ESOMAR/GRBN sobre Investigación Online, la Guía ESOMAR/GRBN sobre Calidad de Muestras Online y la Lista de Comprobación sobre Protección de Datos de ESOMAR donde se describen con más detalle muchas de las recomendaciones y/o requisitos.

A lo largo de este documento el término “debe” se emplea para identificar requisitos obligatorios. Usamos el término “debe” cuando se describe un principio o práctica que los investigadores están obligados a cumplir. El término “debería” se emplea para describir una implementación. El uso de este término indica que los investigadores pueden elegir implementar un principio o práctica de diferentes formas dependiendo del diseño de su investigación.

2 DEFINICIONES

Para el propósito de esta Guía los siguientes términos tienen estos significados específicos:

Actividad ajena a la (o que no es) investigación significa tomar una acción directa hacia un individuo cuyos datos personales han sido recogidos o analizados con la intención de cambiar sus actitudes, opiniones o acciones.

Aviso de privacidad (en ocasiones referido como política de privacidad) significa un resumen publicado de las prácticas de privacidad de una organización y que describen la manera en que una organización recoge, usa, comunica y gestiona los datos personales de un individuo.

Cliente significa cualquier individuo u organización que solicita o contrata un proyecto de investigación.

Cliente misterioso (Mystery shopping) es la recogida de datos en la que se emplean a personas entrenadas para observar, experimentar y medir un proceso de servicio al cliente actuando como un cliente o cliente potencial y adoptando una serie de tareas predeterminadas para evaluar el cumplimiento respecto de estándares de calidad de servicio, o para reunir información sobre ofertas de la competencia.

Consentimiento significa manifestación libre e informada por la que una persona acepta la recogida y tratamiento de sus datos personales.

Daño significa daño tangible y material (como puede ser una lesión física o una pérdida económica), daño intangible o moral (como pueden ser daños a la reputación o clientela, o una intrusión excesiva en la vida privada, incluyendo mensajes individualizados de marketing no solicitados).

Datos de redes sociales significa información (por ejemplo, comentarios o fotos) que generan los usuarios o que comparten mientras interactúan en una red social.

Datos personales (en ocasiones denominado información de identificación personal o IIP) significa cualquier información relacionada con una persona física viva (aquí referida como “el interesado”) que puede usarse para identificar a un individuo, por ejemplo por referencia a identificadores directos (como pueden ser un nombre, una localización geográfica específica, un número de teléfono, una imagen o una grabación de audio o video) o indirectamente por referencia a las características físicas, fisiológicas, mentales, económicas, culturales o sociales de un individuo**.** Una ID de dispositivo y una huella digital también son consideradas como datos personales en algunas jurisdicciones.

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

Datos secundarios significa datos recogidos para otra finalidad y subsecuentemente empleados en la investigación.

Datos sensibles significa cualquier información sobre la raza, origen étnico, salud o vida sexual, antecedentes penales, opiniones políticas o creencias religiosas o filosóficas de un individuo identificable. Puede haber información adicional (por ejemplo, localización o información financiera) que sea definida como sensible en algunas jurisdicciones.

Dispositivo móvil significa un dispositivo pequeño, ligero y que puede ser manejado con la mano (como puede ser un teléfono móvil o una tableta) y que normalmente dispone de una pantalla táctil o de un teclado reducido.

Geolocalización significa la localización geográfica de un dispositivo, como puede ser un ordenador, teléfono móvil, tableta, etc.

GPS (global positioning system) significa cualquier sistema de navegación por satélite que proporciona información sobre la localización y la hora en cualquier situación meteorológica y en cualquier lugar sobre o cerca de la tierra en el que hay una línea ininterrumpida de visión con cuatro o más satélites GPS.

Historial de navegación web significa la lista de páginas web que un usuario ha visitado recientemente -y sus datos asociados como pueden ser el nombre de la página y la hora de visita – y que es registrada por el software del navegador web durante un periodo determinado de tiempo.

Huella digital significa una serie de datos de configuración sobre el dispositivo de un participante (como pueden ser un ordenador, teléfono móvil o tableta) que pueden ser usados para crear la huella digital de la máquina o del dispositivo. Tales sistemas asumen que la "huella digital" identifica de forma unívoca la configuración y características del dispositivo de un usuario asociadas a un dispositivo individual o, potencialmente, la cuenta de usuario de un individuo.

Interesado significa cualquier individuo cuyos datos personales son empleados en una investigación. También se le denomina "titular de los datos".

ID del dispositivo significa un número distintivo asociado a un teléfono móvil o dispositivo móvil similar. El ID de dispositivo es diferente del número de serie del hardware del equipo. El término "ID de dispositivo" se usa frecuentemente en la investigación para describir una "huella digital".

Investigación (que incluye todos los tipos de investigación de mercado, social y de la opinión y el análisis de datos) es la recogida e interpretación sistemática de información sobre personas y organizaciones. Emplea métodos y técnicas estadísticas y analíticas de las ciencias sociales y conductuales aplicadas para generar perspectivas y apoyar en la toma de decisiones a los proveedores de bienes y servicios, gobiernos, ONG's y al público en general.

Investigador significa cualquier individuo u organización que lleva a cabo o actúa como consultor en una investigación, incluyendo a aquellos que trabajan en la organización del cliente y en cualquier subcontratista utilizado.

IoT (Internet de las Cosas) significa la red de dispositivos físicos, vehículos, edificios u otros elementos que incorporan electrónica, software, sensores, activadores y conectividad a la red que permiten a dichos objetos recoger y comunicar datos.

Niños significa individuos para quienes se debe obtener el permiso paterno o de un adulto responsable para participar en una investigación. La definición de edad de un niño varía sustancialmente y es establecida por la legislación nacional y por los códigos de auto-regulación. En ausencia de una definición nacional, se considera niño a los menores de 12 años y "persona joven" a los comprendidos entre los 13 y los 17 años.

Panel de acceso (access panel) se refiere a una base de datos de potenciales entrevistados que declaran que cooperarán en futuras recogidas de datos si son seleccionados.

Paradatos significa datos sobre el proceso en el que se recogen los datos, incluyendo el comportamiento de los interesados durante la recogida de datos.

Recogida de datos pasiva significa la recogida de datos personales mediante la observación, medición o grabación de las acciones o comportamientos de un individuo.

Reconocimiento facial significa método de reconocer los movimientos musculares del rostro de un individuo para inferir sus reacciones emocionales en respuesta a diversos estímulos, como por ejemplo un anuncio publicitario o un nuevo concepto de producto. Esto es diferente de la técnica de reconocimiento facial en el que la finalidad es identificar a un individuo en concreto mediante una imagen digital.

Revelación deductiva significa la deducción de la identidad de un interesado mediante análisis cruzados, el uso de muestras pequeñas o mediante la combinación con otros datos (como pueden ser los registros de un cliente o datos secundarios públicos).

SMS (Short Message Service) significa un servicio de mensajería de texto de un sistema de comunicación por teléfono, web o móvil que emplea protocolos de comunicación estandarizados y que permite el intercambio de mensajes cortos de texto entre dispositivos de teléfono fijos o móviles.

Teléfono móvil (también conocido como teléfono celular o teléfono portátil) significa un dispositivo que puede efectuar y recibir llamadas de teléfono mediante una emisión radiofónica mientras se desplaza por una extensa área geográfica.

Wearables (dispositivos vestibles) significa dispositivos electrónicos (sensores) que se llevan sobre, bajo o como parte de la ropa y capaces de recoger información e intercambiar datos sin intervención humana.

3 INTERESADOS: RELACIONES Y RESPONSABILIDADES

3.1 Asegurar la ausencia de daños

Los investigadores deben tomar todas las precauciones razonables para asegurar que los interesados no se vean perjudicados como resultado del uso de sus datos en una investigación. En este sentido, deben tener en cuenta los requisitos específicos de la investigación; consultar los requisitos o restricciones locales, la legislación y la costumbre; y tomar en consideración las implicaciones prácticas que las actividades de investigación puedan tener sobre los interesados. En todos los casos, los investigadores sólo deben solicitar de los interesados lo que desde el punto de vista de los interesados sea aceptable, seguro y justo.

Los investigadores también deben asegurarse de que cualquier software que proporcionen a los interesados esté comprobado totalmente, cumple con las normas de privacidad acordadas previamente y no interfiere o daña el dispositivo móvil. Véase para más detalle la Sección 6 – Prácticas no aceptables.

3.1.1 Seguridad

Cuando se realizan llamadas telefónicas a dispositivos móviles, los investigadores podrían ocasionalmente contactar con interesados potenciales que estén ocupados en alguna actividad o se encuentren en un entorno que normalmente no suele darse cuando se llama a un teléfono fijo. Esto puede incluir la conducción de un vehículo, el manejo de una maquinaria o mientras se camina en una zona pública. El investigador debe confirmar que el individuo está en una situación en la que es legal, seguro y conveniente atender la llamada. Si el investigador no recibe una confirmación, la llamada debería finalizarse permitiendo la posibilidad de realizar nuevos intentos en otro momento.

Algunos métodos de investigación mediante dispositivos móviles incluyen solicitar a las personas para que recojan datos al visitar lugares concretos o realizando tareas específicas. En tales casos, los investigadores deben prevenirles para evitar que hagan algo que pueda suponerles un riesgo, incumplir la ley o invadir la privacidad de otras personas. Por ejemplo, avisándoles de no escribir texto o interactuar de otra forma con su dispositivo móvil mientras conducen o no tomar fotos o grabaciones en lugares donde esté prohibido (como pueden ser edificios gubernamentales, bancos, colegios, zonas de seguridad aeroportuarias, zonas privadas o aquellas zonas incluso de establecimientos públicos donde exista un aviso que prohíba el uso de cámaras).

3.1.2 Confidencialidad y datos sensibles

Un investigador podría contactar a un interesado potencial que en ese momento esté ocupado, esté realizando una actividad o se encuentre en una situación en la que otras personas puedan escuchar la conversación telefónica. En este caso, el investigador debe tener en cuenta la naturaleza del contenido de la investigación y que el interesado puede ser escuchado inadvertidamente mientras revela información o comportamientos personales, por lo que podría modificar sus respuestas como resultado de su situación. Cuando sea apropiado, la llamada telefónica debería ser reprogramada para otro momento o localización en la que no se ponga en riesgo la confidencialidad.

Los investigadores también deben tener cuidado cuando contacten con interesados sobre temas de naturaleza sensible debido al riesgo de daño o incomodidad. En algunos países puede ser necesario obtener la autorización de la autoridad nacional relevante para recoger datos sensibles.

3.1.3 Costes

A diferencia de otros métodos de investigación, los interesados pueden incurrir en costes derivados de su participación en una investigación mediante dispositivos móviles. Estos costes pueden derivarse de la descarga de datos, acceso online, envío de mensajes, exceso de consumo de planes de datos, cargos por roaming, recuperación de mensajes del buzón de voz, además del coste estándar del teléfono. Los investigadores deberían diseñar su investigación de manera que los interesados no incurran en costes sin su previo consentimiento. Si esto no es posible, los investigadores deben estar preparados para ofrecer alguna compensación. Dicha compensación puede ser en efectivo, dinero electrónico, minutos de voz o de otra manera.

3.1.4 Distinguir entre actividades de investigación y las que no son de investigación

Los investigadores deben asegurarse de que los fines de la investigación se distinguen claramente de aquellas actividades que no son de investigación. Además, no deben permitir que cualquier dato personal que hayan recogido con un fin de investigación sea usado para cualquier otro fin sin el consentimiento previo del interesado. Este requisito no impide a los investigadores involucrarse en actividades que no son de investigación siempre que, cuando recojan datos personales para un fin distinto al de investigación, tal fin sea comunicado expresamente al interesado, se diferencie razonablemente de cualquier actividad de investigación en la que estén participando y se obtenga su consentimiento previo a la recogida de los datos personales para fines distintos de la investigación.

3.2 Niños y otras personas vulnerables

Cuando se lleve a cabo una investigación con niños u otras personas vulnerables, los investigadores deben consultar la legislación nacional y los códigos de auto-regulación en las jurisdicciones donde se recogerán los datos para determinar los casos en que es necesario el permiso parental o cuando las sensibilidades culturales requieren un tratamiento particular. Cuando se contacte por teléfono con un interesado, si es aparente que se trata de un niño, el investigador no debe proseguir con la entrevista a no ser que se obtenga el permiso paternal o de un adulto responsable para invitar al niño a participar en una investigación. Si la persona no está autorizada, algunas jurisdicciones pueden requerir que el investigador ofrezca la oportunidad de participar en la investigación usando otro método.

Los investigadores deben tener especial cuidado cuando fotografíen o graben a niños. Si no es posible obtener el permiso, las imágenes de los niños deben ser pixeladas o borradas.

La mayoría de los sistemas operativos de los dispositivos móviles tienen funciones que permiten, al activarlas, obtener el consentimiento paterno previo antes de instalar la aplicación. Los investigadores deberían usar este tipo de configuración cuando desarrollen o encarguen el desarrollo de una aplicación para ser usada en la investigación.

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

Los investigadores deben obtener el consentimiento de los interesados antes de recoger cualquier tipo de dato personal y deben ser transparentes sobre:

- su identidad;
- la información que tienen previsto recoger;
- el fin general para el que será recogida;
- el método de recogida de datos;
- durante cuánto tiempo se espera que participe el interesado;
- cómo se protegerán los datos; y
- con quién se compartirán los datos y de qué forma.

Esta información debería ser clara, concisa y notoria. Véase también la Sección 3.7.1 Avisos de privacidad. Además, en caso de que alguna de la anterior información cambie, es necesario un nuevo consentimiento del interesado. Los interesados nunca deben ser confundidos, mentidos, engañados o coaccionados. La participación en una investigación es siempre voluntaria y se debe permitir en cualquier momento a los interesados que se retiren de la investigación y que sus datos personales sean cancelados.

Finalmente, los investigadores deben respetar toda la legislación y los códigos de conducta profesionales locales que sean relevantes.

3.3.1 Minimización de datos y carga razonable

Los investigadores deben limitar la recogida y/o tratamiento de datos personales a aquellos elementos que sean relevantes para la investigación. También deberían asegurarse de que cualquier tarea asignada al interesado (por ejemplo, una encuesta, un diario o un foro de discusión) sea presentada en un formato adecuado para un dispositivo móvil y de una longitud adecuada.

El menor tamaño de pantalla de algunos dispositivos móviles implica que se deba tener un cuidado especial para asegurarse de que las instrucciones, las preguntas o los formularios sean claros, legibles y concisos. Esto incluye optimizar el formato entre diferentes dispositivos y excluir ciertos dispositivos cuando la entrevista sea demasiado larga o demasiado compleja para dicho dispositivo. A estas prácticas se les suele denominar mediante términos como “móvil primero”, “agnóstico a dispositivos”, “diseño receptivo” o “diseño adaptativo”.

Aunque la investigación sigue evolucionando, la experiencia actual sugiere que los interesados participantes en una investigación mediante dispositivos móviles esperan una interactuación con los investigadores más breve que en otro tipo de investigación, como puede ser las encuestas telefónicas o los grupos de discusión presenciales.

Se deben aplicar precauciones similares cuando se diseñen encuestas auto-administradas mediante un teléfono móvil, ya que se ha comprobado que en la investigación mediante teléfono móvil es más difícil mantener a los interesados online que en la investigación mediante línea fija de teléfono.

3.3.2 Contactar con interesados potenciales

La tecnología y las comunicaciones móviles han crecido rápidamente mientras que los marcos legales aún están en desarrollo. Tales marcos legales afectan indirectamente, y podrían potencialmente representar una responsabilidad legal para el investigador en el momento de contactar a un interesado mediante un dispositivo móvil, ya sea por vía telefónica, de correo electrónico o por mensaje de texto. Por ejemplo, en algunos países el empleo de sistemas automatizados de envío de mensajes de texto está prohibido salvo que se obtenga el consentimiento explícito.

Los investigadores no deben emplear ningún subterfugio para obtener la dirección de correo electrónico o el número de teléfono móvil de los interesados potenciales. Esto incluye el uso de páginas web públicas, el uso de tecnologías o técnicas sin el conocimiento del individuo o la recogida de datos personales bajo el disfraz de otra actividad distinta a la investigación. Finalmente, las llamadas realizadas a teléfonos móviles deberían identificar el número llamante; esta identificación no debería ser eliminada deliberadamente.

Los investigadores deben verificar con quien suministre la muestra (ya sea un proveedor de muestras o el cliente) que esta contiene sólo individuos que tengan una expectativa razonable de recibir correos electrónicos o mensajes de texto solicitando su participación en una investigación.[1]

[1] Otras tecnologías de mensajería, como pueden ser la notificación de aplicaciones móviles, pueden tener características y funcionalidades similares a las de los mensajes de texto.

Pueden consultarse las prácticas aceptables en la Sección 3.5 de la Guía ESOMAR/GRBN sobre Investigación Online.

3.3.3 Investigación telefónica

Cuando se realicen llamadas a teléfonos móviles los investigadores deben tener en cuenta que, aunque la legislación pueda limitar las llamadas no solicitadas para fines comerciales pero no para fines de investigación, es vital consultar y respetar las listas de exclusión específicas para fines de investigación, tanto de líneas móviles como de fijas.

Algunos países también cuentan con leyes o estándares que especifican las horas en que se pueden realizar llamadas de teléfono no solicitadas de cualquier tipo, legislación que también debe ser respetada para encuestas a teléfonos móviles. Los investigadores deberían tener en cuenta que las personas contactadas pueden encontrarse en zonas con un horario diferente, por lo que deberían verificar la conveniencia de la hora en que llaman, además de su localización y situación. En ausencia de tales requisitos, los investigadores deberían observar las mismas horas de llamada que las empleadas en llamadas a teléfonos fijos. Para la investigación en el sector B2B, las horas aceptables están implícitas en el

horario de oficina del destinatario afectado. Debería prestarse atención también al envío de mensajes a móviles para evitar que los participantes reciban avisos de llegada de un mensaje fuera de las "horas normales".

En algunos países está limitado el uso de sistemas de marcación automática. En otros, está permitido el uso de tales sistemas sólo si el interesado ha dado su consentimiento explícito previamente para ser llamado mediante un sistema de marcación automática (por ejemplo, en el caso de miembros de un access panel). En los casos en que se permite el uso de sistemas de marcación automática, no están permitidas las llamadas abandonadas o silenciosas en las que no hay un entrevistador disponible inmediatamente.

3.3.4 Incentivos

Cuando se ofrezcan incentivos para alentar la participación en la investigación mediante dispositivos móviles, los investigadores deben asegurarse de que se informa claramente a los interesados sobre:

- en qué consistirá el incentivo;
- quién se lo hará llegar;
- cuándo lo recibirán; y
- si está sujeto a condiciones (por ejemplo, completar una tarea específica, dar acceso a una recogida de datos pasiva, superar los controles de calidad, tiempo mínimo de permanencia requerido como miembro activo en una comunidad, etc.).

Los investigadores deberían tener cuidado al usar los incentivos facilitados por el cliente (como podrían ser productos del cliente o artículos con el logo del cliente) ya que en algunas jurisdicciones esto podría considerarse como una actividad de marketing.

Puede consultarse para más detalle sobre incentivos, incluyendo el uso de sorteos la Sección 3.6 de la Guía ESOMAR/GRBN sobre Investigación Online.

3.4 Recogida pasiva de datos

Las aplicaciones móviles pueden recoger una amplia gama de datos personales sin la participación directa de los interesados. Por ejemplo, uso de páginas web e historial de navegación, estadísticas de uso de aplicaciones, datos de tarjetas de fidelización, geolocalización, datos de redes sociales, datos de wearables (dispositivos vestibles) e IoT y otros datos generados u obtenidos de los dispositivos móviles.[2]

[2] Aunque es posible detectar pasivamente el tipo de dispositivo que está usando un interesado, esto no es un dato personal siempre que la finalidad sea optimizar el funcionamiento de la aplicación y el desarrollo de la encuesta.

Adicionalmente, algunas tecnologías específicas, como puede ser el tracking online, tienen una aplicación válida en la investigación mediante recogida pasiva de datos y que normalmente incluye:

- mejoras en la integridad de las muestras online;
- prevención del fraude; o
- aplicaciones de investigación, incluyendo y sin limitarse a: medición de audiencias online, medición de contenidos y tests publicitarios.

En estas circunstancias u otras similares, los investigadores deben hacer todos los esfuerzos necesarios para obtener el consentimiento descrito en la Sección 3.3. Cuando no sea posible obtener el consentimiento (como puede ser al medir el tráfico de una página web), los investigadores deben tener una base legal para recoger los datos y deben eliminar u ocultar cualquier información de identificación tan pronto como sea operativamente posible (véase la Sección 3.7.2 Desidentificación de los datos).

3.4.1 Datos biométricos

La recogida pasiva y la recogida de datos de comportamiento también pueden implicar interacciones directas con los interesados. Por ejemplo, el reconocimiento facial implica la grabación de la cara del interesado mientras éste completa una encuesta o realiza una tarea similar. Los dispositivos de seguimiento de ojos, los cascos de realidad virtual y otros dispositivos vestibles (wearables) pueden usarse de forma similar. Todos estos pueden implicar la recogida de datos personales y, en algunos casos, datos que pueden clasificarse como sensibles en algunas jurisdicciones, siendo necesario establecer procesos para verificar el cumplimiento de la legislación local aplicable y de los códigos sectoriales.

3.4.2 Fotografías y grabaciones

Las fotografías y las grabaciones de audio o video son datos personales y, por tanto, deben ser recogidas, tratadas y conservadas como tales. Sólo pueden compartirse con un cliente si el interesado ha dado su consentimiento previo e informado de la finalidad específica para la que serán usados. Cuando se haya eliminado información potencial de identificación de forma que ya no sea considerado dato personal (como puede ser mediante el pixelado o empleando tecnologías de distorsión de la voz) puede compartirse con el cliente, siempre que el cliente acuerde no realizar ningún intento de identificar a los individuos.

Los investigadores no deben instruir a los interesados (o a aquellos que realicen la recogida de datos) a participar en actividades de seguimiento de individuos o de lugares públicos. A los interesados se les debería asignar tareas específicas limitadas (por ejemplo, captar escenas con amigos con su consentimiento, o imágenes de objetos o escaparates) que no impliquen la monitorización de una zona en concreto en la que se puedan captar datos personales sin el consentimiento de los individuos presentes. Cuando se lleve a cabo una observación mediante grabación en un local público, deberían colocarse señales claras y legibles indicando que la zona está bajo observación, junto con los detalles de contacto del investigador o de la organización que realiza la investigación, y las imágenes de los individuos deben ser pixeladas o borradas lo antes posible. Las cámaras deberían estar situadas de forma que monitoricen solo las áreas donde se pretenda realizar la observación.

3.4.3 Seguimiento en tienda

El seguimiento en tienda de interesados es una forma de recogida de datos pasiva en la que se registra el movimiento de los individuos dentro de la tienda mientras realizan sus compras. Las aplicaciones específicas pueden ser de dos categorías genéricas.

En la primera categoría, se solicita a los interesados que porten un dispositivo o que se descarguen una aplicación que se sincroniza con el hardware (como puede ser una baliza) para seguir y registrar el movimiento dentro de la tienda. En esta categoría son de aplicación los requisitos estándar sobre notificación y consentimiento (véase la Sección 3.3 - Notificación, honestidad, consentimiento y la naturaleza voluntaria de la investigación).

En la segunda categoría, puede no haberse informado explícitamente a los interesados de que están siendo observados y de que se están recogiendo datos de comportamiento mientras se encuentran en la tienda. En estos casos, los investigadores deben asegurarse de que:

- la monitorización y la recogida de datos está permitida por la legislación local;
- existe una clara señalización indicando que se está registrando el comportamiento; y
- cualquier información de identificación sea eliminada u ocultada tan pronto como sea operacionalmente posible.

3.5 Cliente misterioso (Mystery shopping)

Los interesados (normalmente se trata de trabajadores) en un estudio de tipo mystery shopping normalmente no son conscientes de que están siendo observados. Los investigadores deben tener cuidado de que se respete la privacidad individual y de que los interesados no se vean en desventaja o perjudicados de cualquier forma como resultado de ser objeto de un ejercicio de un estudio de tipo mystery shopping. Se deben proteger sus datos personales y no deben compartirse con el cliente fotografías o grabaciones, salvo que se cuente con el permiso para ello de los interesados, normalmente como parte de una relación laboral.

La investigación mediante mystery shopping es diferente de la recogida inmediata de datos diseñada para capturar la reacción de un interesado ante experiencias de compra y su influencia en la decisión de compra, que es un método de investigación etnográfica realizada con su consentimiento.

3.6 Uso de datos secundarios

En esta era digital se está generando una creciente cantidad de datos derivados incidentalmente de los resultados de las actividades y transacciones habituales del día a día. Por ejemplo, los proveedores de servicios de telefonía móvil frecuentemente recogen una extensa información sobre sus clientes y el uso que hacen de los dispositivos móviles. Los teléfonos móviles registran no solo a quién se llama y quién llama, sino también datos de geolocalización de dónde han estado, páginas web que han visitado, a qué puntos de la red de telefonía se ha conectado su dispositivo, etc. También pueden registrar información sobre el uso de aplicaciones individuales e incluso datos relativos a mensajes publicados en redes sociales.

Estos y otros datos similares representan nuevas oportunidades para los investigadores para ampliar su comprensión del comportamiento de las personas. Aunque los investigadores en ocasiones diseñan proyectos para recoger algunos de estos tipos de datos empleando métodos tradicionales, la mayor parte de estos datos ya existen como datos secundarios que pueden estar disponibles para su reutilización.

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

- el uso planificado está permitido legalmente conforme a los términos acordados con los interesados antes de la recogida de datos y que no están específicamente excluidos en los avisos de privacidad en el momento de su recogida original;
- los datos no hayan sido recogidos incumpliendo las restricciones legales, mediante engaño o de forma que su recogida no fuera aparente o razonablemente discernible y anticipada por el interesado;
- los interesados tengan una expectativa razonable de que los datos pueden ser empleados para otros fines, como puede ser fines de investigación;
- se atiende cualquier solicitud de los interesados para que sus datos no sean usados para otros fines; y
- la organización que suministra los datos tiene legalmente el derecho a compartirlos.

Los investigadores también deben tener en cuenta si el tratamiento ulterior de los datos puede implicar un riesgo que cause un daño a los interesados mediante su revelación por deducción. Si existe tal riesgo, los investigadores deben emplear salvaguardias para mitigar el riesgo de tales daños. Esto incluye, pero sin limitarse a ello, asegurarse de que la identidad de los interesados no sea revelada o descubierta sin su consentimiento previo y que no se les dirigirán actividades ajenas a la investigación como consecuencia directa de que sus datos sean empleados en una investigación.

3.7 Protección de datos y privacidad

Los investigadores deben adoptar principios[3] universales de protección de datos personales. Estos principios establecen que cualquier dato personal recogido o usado debe ser:

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

- recogido para una finalidad específica y no usado de manera incompatible con dicha finalidad;
- adecuado, relevante y no excesivo en relación a la finalidad para la que es recogido y/o tratado;
- no es recogido incumpliendo las restricciones legales, mediante engaño o de forma que no sea aparente o razonablemente discernible, o no pueda ser anticipado por los interesados;
- no usado de forma que pueda provocar daño a los interesados, incluyendo la adopción de medidas para prevenir dichos daños;

- protegido ante el riesgo de pérdida, acceso, destrucción, uso, manipulación o revelación no autorizadas; y

- conservado durante un plazo no superior al necesario para la finalidad para la que se recogió o trató la información.

Los investigadores disponen de diversos estándares y marcos regulatorios para desarrollar políticas y normas de seguridad de los datos. Para más información, los investigadores pueden consultar ISO 27001: Tecnología de la Información – Técnicas de seguridad – Sistemas de Gestión de Seguridad de la Información - Requisitos o la Lista de Comprobación de Protección de Datos de ESOMAR.

Los investigadores deben tener cuidado cuando decidan almacenar datos personales en la nube. Deben evaluar los controles de seguridad del proveedor del servicio de alojamiento en la nube y sus términos y condiciones estándar, y estar preparados para implementar controles complementarios si los controles del proveedor no son suficientes. Para más detalle, consultar la Sección 7.7 de la Guía ESOMAR/GRBN sobre Investigación Online, la Lista de Comprobación de Protección de Datos de ESOMAR, y la Guía Práctica de Cloud Computing.

3.7.1 Avisos de privacidad

La legislación sobre privacidad normalmente requiere que las empresas de investigación pongan a disposición de los interesados un aviso de privacidad. Debido a la limitación derivada del tamaño de pantalla de los dispositivos móviles, los investigadores deberían considerar el uso de avisos de privacidad organizados por capas. Esto normalmente consiste en un aviso corto que contiene la información básica, como puede ser la identidad de la organización y la forma en que se usarán los datos, más un aviso más extenso en una segunda capa.

Los interesados deben disponer de suficiente información basada únicamente en los avisos cortos para manifestar su consentimiento. Este aviso corto debe destacar los usos de los datos que no sean obvios (como podrían ser el sonido o la imagen, la geolocalización), el uso secundario, si se comparten los datos, la conservación de los datos; en lugar de los tipos obvios de datos recogidos como el nombre, edad y las opiniones.

El aviso corto debería contener un vínculo a una segunda capa con una descripción más detallada. Toda la información debe ser fácilmente visible sin necesitar desplazarse por ventanas diseñadas para ser visionadas en un ordenador de sobremesa.

El aviso de privacidad debe incluir una declaración sobre la legislación conforme a la cual se recogen los datos. Si se recogen datos en diversos países, el investigador debe cumplir la legislación de los países donde se desarrolla la investigación. Cuando sea posible conocer el país de residencia de los interesados, los investigadores deben cumplir los requisitos legales de dicho país, teniendo en cuenta que pueden existir diferencias considerables entre distintas jurisdicciones.

3.7.2 Desidentificación de los datos

Los investigadores deben asegurarse de que cualquier dato compartido con los clientes u otros usuarios de datos está suficientemente desidentificado para evitar la revelación de datos personales. Existe una variedad de técnicas de desidentificación, y cada una aporta diversos niveles de protección frente a la revelación de datos personales y/o medidas de seguridad adicionales. Estas técnicas abarcan un amplio rango de medidas de manipulación de datos que incluyen la eliminación de identificadores directos, la eliminación de identificadores indirectos (elementos que potencialmente permiten la revelación deductiva) y la transformación de los datos (por ejemplo, el troceado, la encriptación o la agregación).

La seudonimización es una técnica popular para desidentificar datos durante su tratamiento y para cuando sea necesario reidentificar los datos para fines como la validación o la comparación. Normalmente implica la separación de los datos personales de los datos de la investigación, manteniendo ID’s diferentes en cada fichero, y creando un tercer fichero que vincula ambos ID’s el cual puede ser usado para reconstruir los datos originales cuando sea necesario. El acceso al fichero con la vinculación debe estar limitado sólo a personas determinadas. Se recomienda encarecidamente a los investigadores que utilicen la seudonimización en los datos tan pronto como sea posible tras su obtención.

La anonimización implica una variedad de técnicas en las que los datos personales son borrados o modificados de forma que no sea posible la posterior reidentificación de los interesados, ni siquiera por medio de revelación deductiva. Algunos ejemplos son: eliminar o encriptar los datos individuales, difuminar las imágenes para esconder la cara en fotografías y videos, introducir ruido o sólo entregar los resultados de la investigación en forma de agregación estadística.

3.7.3 Seguridad del dispositivo

Los datos personales almacenados localmente en el dispositivo móvil del interesado pueden estar potencialmente a disposición de terceros en caso de que el dispositivo sea robado o utilizado por otra persona. Por ejemplo, los datos almacenados en aplicaciones para investigación, o no, que estén instaladas en el dispositivo; fotografías tomadas en el contexto de un estudio etnográfico o en otras actividades de investigación; y SMS, correo electrónico u otros tipos de mensajes que puedan haber sido usados para transmitir los datos de la investigación y que incluyan datos personales.

Cuando se recojan datos de wearables u otros dispositivos de IoT, los investigadores deben asegurarse de que todos los datos sean encriptados antes de su transferencia entre dispositivos.

Se debe informar a los interesados de estos riesgos y los investigadores deben implementar medidas para proteger los datos personales. Por ejemplo, la encriptación de los datos (incluyendo la encriptación de los datos en depósito y los que están en tránsito), protección del dispositivo mediante una contraseña, suministrando a los interesados instrucciones de cómo borrar toda la información personal a la finalización de la investigación, y otros tipos de medidas de seguridad o de control.

3.7.4 Uso de ID’s estáticas y dinámicas

Los clientes de la investigación y los proveedores de muestras ocasionalmente usan identificadores estáticos para los interesados (ID’s estáticos) para ayudar al control y asignación de interesados en estudios ad hoc o continuos. Esta técnica permite consolidar la información sobre cada interesado y supone un mecanismo útil para asegurar que los mismos interesados participen en un estudio continuo y/o que se cumplan los periodos de carencia de participación en una investigación.

Algunos proveedores de muestras prefieren las ID’s dinámicas (ID’s variables para cada uso) para proteger la identidad de los interesados.

Los investigadores deberían tener en cuenta el uso de cada tipo de ID, equilibrando la privacidad de los interesados con los requisitos de calidad en el contexto de cada estudio específico.

3.7.5 Uso y controles de los paradatos

Los investigadores solo deben usar los paradatos cuando exista un acuerdo legal entre el proveedor de muestras y el cliente que oriente, limite y proteja la recogida, uso y posterior transferencia de estos datos sobre el proceso de recogida de datos en las actividades de investigación y análisis. En algunas jurisdicciones los paradatos son considerados datos sensibles.

3.7.6 Transferencias transfronterizas

Antes de que los datos sean transferidos desde el país de recogida a otro país, el investigador debe asegurarse de que la transferencia de datos es legal y de que se han tomado todas las medidas razonables para asegurar la privacidad y seguridad de dichos datos. Esto es aplicable si un servidor de recogida de datos está ubicado en un país distinto de el del interesado. También será de aplicación si se emplea tecnología en la nube para el almacenamiento de datos en otro país.

El investigador debe conocer la legislación aplicable en los países de origen y de destino relativa a la protección de datos en caso de transferencia transfronteriza, teniendo en cuenta que pueden existir mecanismos alternativos para facilitar la transferencia de datos.

3.7.7 Notificación de violaciones en la seguridad

Los investigadores deben cumplir la legislación relevante en relación a la notificación de violaciones en la seguridad y en relación a los requisitos de los países donde se recogen los datos. Los investigadores deben

comunicar las violaciones en la seguridad y en los datos a la autoridad relevante cuando exista, y después a todas las partes afectadas incluyendo clientes, interesados y subcontratistas sin demora indebida. La notificación debería incluir una descripción de los tipos de datos afectados por la violación en la seguridad y las medidas que los interesados deberían adoptar para protegerse a sí mismos de daños potenciales resultantes de la violación en la seguridad.

3.8 Compartir datos personales con un cliente

Salvo que la legislación aplicable establezca un requisito superior, si los investigadores tienen previsto recoger datos personales para una investigación que también puedan ser usados para fines ajenos a la investigación, debe informarse a los interesados antes de la recogida de datos y debe obtenerse su consentimiento para los fines ajenos a la investigación.

Los investigadores no deben compartir los datos personales de identificación de un interesado con un cliente a menos que el interesado haya dado su consentimiento para ello y esté de acuerdo con la finalidad específica para la que serán usados.

Incluso cuando se entreguen al cliente datos anonimizados, los investigadores deben obtener del cliente una garantía por escrito de que éste no intentará reidentificar a los interesados salvo que se cumplan las condiciones anteriores.

3.8.1 Observadores

Algunos tipos de investigación incluyen casos en que los individuos puedan tener acceso a datos personales mediante la observación de la recogida de datos en tiempo real o posteriormente mediante video o una interfaz gráfica del cliente. Esto puede ser el caso de las personas del equipo del cliente que no son investigadores o subcontratistas del cliente (por ejemplo, las agencias de publicidad).

En tales casos, los investigadores deben obtener:

- el consentimiento de los interesados para ser observados por tales personas (incluyendo su afiliación) durante o tras la recogida de datos; y
- un acuerdo formal de todos los clientes y otros observadores de abstenerse de revelar los datos personales de los interesados o de usarlos de cualquier forma distinta de los fines de investigación sin consentimiento.

4 CLIENTES: RELACIONES Y RESPONSABILIDADES

4.1 Subcontratación

Los investigadores deberían informar a los clientes antes de comenzar el trabajo, de los casos en que cualquier parte del mismo vaya a ser subcontratada fuera de la propia organización que lleva a cabo la investigación. Se debe informar a los clientes que lo soliciten de la identidad de tales subcontratistas.

En caso de que la identidad del subcontratista que suministra las muestras pueda ser considerada legítimamente como información reservada, el proveedor de muestra debe proporcionar:

- una descripción del tipo de fuentes de muestras que utiliza; y
- una estimación del porcentaje de la muestra que procederá de un panel y de la que procederá de otras fuentes.

Los investigadores también deben asegurar que los datos personales compartidos con un subcontratista se limitan a los necesarios para llevar a cabo las tareas subcontratadas; que el subcontratista cuenta con los procedimientos de seguridad necesarios para la protección de los datos; y que están claramente documentadas y acordadas las responsabilidades del subcontratista relativas a la protección de datos.

4.2 Calidad metodológica

Si se espera que los usuarios de la investigación mediante dispositivos móviles confíen en que los resultados son adecuados a su propósito, entonces los investigadores deben poner a disposición de los clientes la información apropiada sobre cómo se llevó a cabo la investigación, de forma que les permita evaluar la validez de los resultados incluyendo cualquier limitación de la metodología que pueda conducir a conclusiones no soportadas por los datos. Esta información debería incluir:

- tamaño de la muestra, fuente y cómo se gestionó;
- diseño y selección de la muestra;
- el método de recogida de datos;
- cualquier edición de datos, ponderación o ajustes post-campo que puedan haberse aplicado; y
- cuando la penetración de la telefonía móvil sea inferior al 100%, las medidas adoptadas para asegurar que los resultados de la investigación representan a la población objeto de estudio.

Se pueden consultar los requisitos específicos sobre estos aspectos en la Guía ESOMAR/GRBN sobre Calidad de Muestras Online y en la Sección 6 de la Guía ESOMAR/GRBN sobre Investigación Online.

4.3 Transparencia, distorsión y corrección de errores

Todos los resultados de los proyectos de investigación deben ser comunicados y documentados con precisión, transparencia y de forma objetiva. En caso de que se detecten errores tras la entrega de resultados, se debe informar al cliente inmediatamente y se deben realizar las correcciones lo antes posible.

5 EL PÚBLICO EN GENERAL: RELACIONES Y RESPONSABILIDADES

5.1 Mantener la confianza del público

Los investigadores deben ser honestos, sinceros y objetivos y deben asegurarse de que su investigación se lleva a cabo conforme a principios, métodos y técnicas de investigación científicas apropiadas. Los investigadores deben comportarse siempre de manera ética y no deben hacer nada que pueda dañar la

reputación de la investigación de mercado, social y de la opinión y del análisis de datos. Deben ser siempre conscientes de los principios de los Códigos de CCI/ESOMAR y GRBN en su trabajo, evitando actividades y prácticas que puedan socavar la confianza del público.

5.2 Publicación de los resultados

Para más detalle sobre las responsabilidades del investigador cuando el cliente tiene intención de publicar los resultados de la investigación, véase la Sección 5.2 de la Guía ESOMAR/GRBN sobre Investigación Online.

6 PRÁCTICAS NO ACEPTABLES

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

- no hayan sido testadas en profundidad;
- modifiquen la configuración del dispositivo móvil más allá de lo necesario para realizar la investigación, sin el consentimiento del interesado;
- causen conflictos con el sistema operativo o causen que otro software instalado funcione de manera errática o de forma no esperada;
- estén ocultas con otro software que pueda ser descargado o que sea difícil de desinstalar;
- suministren contenidos publicitarios, con la excepción de lo que sea necesario para una investigación sobre publicidad legítima;
- cambien los datos recogidos sin informar al interesado y sin darle la oportunidad de darse de baja;
- requieran un consumo inusualmente elevado de la batería del dispositivo, salvo que se obtenga el consentimiento específico;
- impliquen un coste para el interesado sin su consentimiento y sin que sea reembolsado por el investigador;
- usen software de geolocalización sin el consentimiento del interesado;
- transmitan datos personales que no estén encriptados;
- cambien la naturaleza de cualquier tecnología de seguimiento e identificación sin notificarlo y sin obtener el consentimiento del interesado;
- no notifiquen al interesado los cambios en la política de privacidad derivados de una actualización;
- recojan datos personales que puedan ser usados por el proveedor de la aplicación para fines ajenos a la investigación sin consentimiento; o
- extraigan información del dispositivo o teléfono móvil, salvo cuando dicha información sea parte de la finalidad del estudio y se obtenga el consentimiento.

A la finalización de la investigación, cualquier aplicación que ya no sea necesaria debe ser desactivada. Los interesados deben ser informados y recibir instrucciones de cómo eliminar la aplicación de sus dispositivos de forma segura.

7 EQUIPO DEL PROYECTO

- Reg Baker, ESOMAR co-chair, Executive Director, MRII and PSC consultant, USA
- Guy Rolfe, GRBN co-chair, Mobile Practice Leader, Innovation & New Technology, Kantar, UK
- Mario Callegaro, Senior Survey Research Scientist, Google, UK
- Simon van Duivenvoorde, Chief Commercial Officer, Wakoopa, NL

- Steve Gutterman, CEO of Mobile Accord, Inc., USA
- Betsy Leichliter, Leichliter Associates, LLC, USA
- Oriol Llaurado, Chief Privacy Officer, Netquest, Spain
- Peter Milla, Consultant to Insights Association, USA
- Paul Quinn, Senior Director, Product Management, Confirmit, UK
- Lisa Salas, Head of Marketing and Operations, TEG Rewards, Australia
- Michael Schlueter, Associate Director Global Innovation, GfK, UK
- Navin Williams, CEO, Mobile Measure, Singapore

ESOMAR: Kathy Joe, Director International Standards and Government Affairs and Jan Willem Knibbe, Policy & Industry Projects Executive