

DIRETRIZES ESOMAR PARA PESQUISAS ONLINE

Material traduzido, discutido e adaptado pelo Conselho de Autorregulamentação da ABEP e elaborado com base nas leis brasileiras.

Todos os códigos e diretrizes da World Research publicados pela ESOMAR, inclusive as mais recentes atualizações, estão disponíveis online no website www.ESOMAR.org

DIRETRIZES ESOMAR PARA PESQUISAS ONLINE

Estas diretrizes serão atualizadas regularmente, conforme necessário. Também estão disponíveis como um documento na internet com links ativos para outras diretrizes publicadas pela ESOMAR e outras fontes. Para visualizar estas diretrizes online, acesse a seção Conhecimento e Padrões, códigos e diretrizes (*Knowledge and Standards, codes and guidelines*) em nosso website, www.ESOMAR.org.

ÍNDICE

1.	INTRODUÇÃO	3
1.1	Princípios gerais para pesquisas online	3
2.	QUESTÕES ÉTICAS	4
2.1	Manipulando dados pessoais	4
2.1.1	Identificadores pessoais	4
2.2	Notificações e e-mail	4
2.2.1	Exigências específicas	4
2.3	Políticas de privacidade	5
2.3.1	Conteúdo recomendado	5
2.4	Crianças e jovens/menores de idade	7
2.4.1	Obtendo permissão	7
3.	QUESTÕES REGULATÓRIAS	8
3.1	Dados pessoais e endereços de IP	8
3.2	Jurisdição nacional	8
3.2.1	Coleta de dados à distância e transferência de dados	8
3.3	Registro	9
3.4	Segurança	9
3.4.1	Gerenciando a segurança	9
4.	UTILIZANDO TECNOLOGIAS ONLINE EM PESQUISAS	10
4.1	Tecnologias de identificação e rastreamento para pesquisas	10
4.1.1	Tecnologias específicas	10
4.1.2	Declaração sobre tecnologias de identificação e rastreamento	11
4.2	Práticas que organizações de pesquisa devem adotar	11
4.3	Práticas inaceitáveis	12
4.4	Aparelhos interativos de telefonia móvel e <i>smartphones</i>	13
4.4.1	Utilizando aparelhos interativos de telefonia móvel	13
5.	QUESTÕES METODOLÓGICAS	14
5.1	Amostras online	14
5.2	Painéis de acesso	14
5.3	Detalhes técnicos	14
6.	DEFINIÇÕES E FONTES DE INFORMAÇÕES ÚTEIS	14
APÊNDICE 1 – Princípios-chave do Código ICC/ESOMAR		16
APÊNDICE 2 – Exemplo de política de privacidade		16

1. INTRODUÇÃO

O [Código Internacional ICC/ESOMAR](#) em Pesquisa de Mercado e Pesquisa Social é neutro em relação a tecnologias e aplica-se plenamente tanto a pesquisas online quanto a qualquer outra forma de coleta de dados. Portanto, os princípios-chave definidos no Código ICC/ESOMAR (veja o [Apêndice 1](#)) formam a base para este documento.

Apesar de muitas das questões técnicas e metodológicas envolvidas na pesquisa pela internet terem sido esclarecidas desde a última atualização destas Diretrizes, em 2005, a estrutura legal internacional regendo a internet ainda está evoluindo, o que significa que a pesquisa online opera em uma estrutura legal não tão bem definida quanto outras formas de pesquisa, especialmente em estudos multipaíses. O objetivo destas diretrizes, portanto, é explicar como aplicar alguns dos princípios fundamentais do Código no contexto dos ambientes legais e regulatórios atuais ao redor do mundo e oferecer suporte para pesquisadores ao tratarem das considerações legais, éticas e práticas envolvidas no uso de novas tecnologias.

A ESOMAR considera igualmente fundamental enfatizar a diferença entre pesquisa de mercado e promoção/vendas. Pesquisa de mercado não é uma comunicação comercial. A distinção pode ser facilmente explicada: dados pessoais coletados para pesquisa de mercado são utilizados exclusivamente para propósitos de pesquisa e não são divulgados para marketing direto ou para outros usos. Veja o Guia ESOMAR [Diferenciando pesquisa de mercado de outras atividades de coleta de dados](#).

A ESOMAR trabalhou em parceria com o CASRO (Conselho Americano de Organizações de Pesquisa) para desenvolver estas diretrizes e, em particular, a seção sobre a utilização de tecnologias em pesquisa está fundamentada e alinhada às orientações do CASRO.

A revisão deste documento ainda está sendo efetuada, sendo que as diretrizes sobre Painéis Online, na seção 5.2, serão definidas em breve. Também se pretende incluir diretrizes sobre outros assuntos relevantes.

1.1 Princípios gerais para pesquisas online

Com leis variando de país a país e novas possibilidades surgindo regularmente, deve haver **três princípios gerais norteando pesquisadores que conduzem levantamentos online. São eles:**

1º) Trate o entrevistado (ou a pessoa que está disposta a participar de uma pesquisa) com respeito. Pesquisadores devem criar um relacionamento com o público baseado em confiança, respeito e reciprocidade, garantindo que as pessoas que participarem de uma pesquisa online tenham uma boa experiência.

2º) Pesquisadores devem ter sensibilidade às preocupações do consumidor e atenção ao fato de que o êxito da pesquisa de mercado depende da confiança do público. Além disso, cabe a estes profissionais evitar atividades e práticas tecnológicas que possam prejudicar a confiança do público na pesquisa de mercado.

3º) Cabe aos pesquisadores preservar a distinção entre pesquisa e atividades comerciais, tais como marketing direto ou promoção/vendas. Quando pesquisadores estiverem envolvidos em atividades que utilizam técnicas de pesquisa, tais como entrevistas, mas que não se destinam exclusivamente para propósitos de pesquisa, não deverão descrever tais atividades como pesquisa de mercado, pesquisa social ou pesquisa de opinião.

Além disso, pesquisadores devem cumprir as exigências de proteção de dados no Artigo 7c do Código Internacional ICC/ESOMAR em Pesquisa de Mercado e Pesquisa Social, que são:

Informações pessoais coletadas e arquivadas, segundo este Código deverão ser:

- *coletadas para propósitos de pesquisa específicos e não utilizadas de forma incompatível com tais propósitos;*
- *adequadas, relevantes e não excessivas, em relação ao propósito da pesquisa para a qual são coletadas e/ou adicionalmente processadas; e,*
- *arquivadas pelo tempo necessário para o propósito para o qual as informações foram coletadas ou adicionalmente processadas.*

Pesquisadores deverão certificar-se de que a identidade pessoal dos entrevistados seja omitida ao cliente. O pesquisador só poderá comunicar informações pessoais do entrevistado ao cliente sob as seguintes condições:

- o entrevistado tenha expresso e registrado sua vontade explicitamente e/ou*
- o entrevistado tenha dado seu consentimento explícito e registrado e*
- pelo entendimento de que nenhuma atividade comercial (conforme definido no Artigo 1d do Código Internacional ICC/ESOMAR em Pesquisa de Mercado e Pesquisa Social) será direcionada a eles como resultado direto das informações que forneceram.*

2. QUESTÕES ÉTICAS

2.1 Manipulando dados pessoais

Os dados fornecidos por entrevistados são confidenciais e a identidade dos entrevistados deve ser protegida. Portanto, ela não deve ser revelada ao usuário das informações sem o consentimento explícito dos entrevistados e o pesquisador deverá certificar-se de que as informações sejam coletadas para os propósitos de pesquisa especificados e não utilizadas de forma incompatível com tais propósitos (veja o Artigo 7 do [Código Internacional ICC/ESOMAR](#)).

Nenhuma informação que possa ser identificada pessoalmente poderá ser utilizada para propósitos não relacionados à pesquisa, tais como marketing direto, mailing, classificação de crédito, arrecadação de fundos ou outras atividades de marketing. (veja o Artigo 1d das [Notas](#) do Código Internacional ICC/ESOMAR).

2.1.1 Identificadores pessoais

O endereço de e-mail do entrevistado ou outros identificadores pessoais (ex. login e senha) são dados pessoais e devem ser protegidos da mesma forma que outros identificadores.

Se todos os dados que podem identificar o indivíduo forem removidos dos registros, o conjunto deixa de conter dados pessoais e não está mais sujeito às exigências de proteção e leis de privacidade.

2.2 Notificações e e-mail

Pesquisadores devem estar atentos às políticas de privacidade e intrusão e não devem efetuar abordagens através de e-mails não autorizados a entrevistados em potencial, mesmo em países onde ainda seja permitido pela lei. A exceção está nos casos em que os indivíduos estejam esperando ser contatados para pesquisas via e-mail.

Pesquisadores devem reduzir qualquer inconveniente que tal e-mail possa causar ao destinatário declarando claramente seu propósito no cabeçalho de assunto e mantendo a mensagem total o mais breve possível.

A mesma exigência aplica-se a outras mensagens eletrônicas (mensagens instantâneas, SMS, etc.). Veja a [seção 4.4](#) sobre aparelhos de telefonia móvel interativos/smartphones.

2.2.1 Exigências específicas

O princípio geral é que pesquisadores de mercado não utilizarão e-mails não autorizados para recrutar entrevistados para propósitos de pesquisa, tanto com consumidores como com empresas (*business-to-business*).

Pesquisadores são obrigados a verificar se os indivíduos contatados para participar de pesquisas por meio de e-mails estejam esperando receber um contato para pesquisa. Tal acordo pode ser presumido quando **todas** as condições a seguir existirem:

- i. Exista um relacionamento pré-existente substancial entre os indivíduos contatados e a organização de pesquisa, o cliente ou os proprietários da lista que compõe a amostra da pesquisa (os últimos sendo desta forma identificados);
- ii. Indivíduos estejam esperando receber um contato para participação em pesquisas, baseado no relacionamento pré-existente;
- iii. Indivíduos tenham a opção de serem excluídos de futuros contatos eletrônicos de uma forma clara, gratuita e de fácil implementação;
- iv. O mailing exclua todos os indivíduos que tenham solicitado sua exclusão da lista.

Pesquisadores não devem utilizar qualquer subterfúgio para obter endereços eletrônicos de entrevistados em potencial, tais como coletar endereços de e-mail de domínios públicos ou sob o pretexto de alguma outra atividade, ou utilizando tecnologias ou técnicas para coletar endereços de e-mail sem o conhecimento dos indivíduos.

Pesquisadores não devem utilizar endereços de e-mail falsos ou enganosos para responder ou recrutar entrevistados pela internet.

Para pesquisas *business-to-business*, o convite para participar da pesquisa poderá ser enviado até mesmo para e-mails não autorizados, desde que os pesquisadores cumpram os pontos 3 e 4 acima e as políticas anti-spam de seus fornecedores de serviços de internet e e-mail. Isso também se aplica a endereços de e-mail de profissionais cujos detalhes tenham sido publicados em domínio público, como por exemplo, listas de médicos ou advogados.

Ao receber mailing de clientes ou proprietários das listas, pesquisadores devem obter do cliente ou fornecedor da lista a confirmação por escrito e/ou alguma documentação de que os indivíduos listados estejam esperando receber contatos por e-mail, conforme definido acima.

É uma boa prática para pesquisadores manter cópias de e-mails e outros documentos recebidos de entrevistados concordando ou restringindo o uso de suas informações pessoais. Essa é uma exigência legal em alguns países, dentre os quais todos os estados-membros da UE (União Europeia), Argentina, Austrália, Canadá, Nova Zelândia e empresas americanas que participam do acordo *U.S.–EU Safe Harbour Framework*.

2.3 Políticas de privacidade

Pesquisadores devem publicar uma declaração de política de privacidade em seu website. Tal declaração deve ser clara, concisa e destacada.

2.3.1 Conteúdo recomendado

A política de privacidade deve ser disponibilizada na forma de um link em todas as pesquisas online e informar, aos participantes da pesquisa, como seus dados pessoais serão utilizados e mantidos em segurança, além das condições sob as quais poderão ser divulgados a um terceiro. Alguns elementos da política serão padrão para todos os levantamentos (**veja a seção A, elementos-padrão para todas as declarações de privacidade**). Outros aspectos variarão dependendo dos métodos de amostragem utilizados (**veja a seção B, três elementos adicionais**). Também pode haver necessidade de incluir antecipadamente no convite para participar de pesquisas online a divulgação de privacidade relacionada a informações relevantes vindas de um levantamento em particular, além das declarações mais gerais na política de privacidade.

A ordem e formulação da política de privacidade é uma questão de escolha. A ESOMAR recomenda que empresas considerem utilizar uma notificação de privacidade em três níveis. Primeiro resumindo, de forma concisa, a política de privacidade; em seguida oferecendo uma breve visão geral das práticas de privacidade de pesquisa de mercado e da empresa; por fim, fornecendo a política de privacidade completa da empresa. Um exemplo de notificação de privacidade em níveis é fornecido no [Apêndice 2](#).

A. Elementos-padrão para todas as políticas de privacidade

Declaração de **quem** está conduzindo a pesquisa, que pode ser acompanhada de link para a página da empresa de pesquisa na internet, onde é possível encontrar mais informações.

Para quem a pesquisa está sendo conduzida: explicitar a identidade da empresa/organização para a qual a pesquisa está sendo executada, a menos que haja boas razões para não fornecer estas informações. Mesmo nos casos de fornecimento de trabalhos de campo ou de processamento, a identificação deverá seguir as instruções adicionais sobre essa questão. Veja [notas](#) sobre como aplicar o Código Internacional ICC/ESOMAR no Artigo 4.

Garantia de que as identidades dos entrevistados e suas respostas serão tratadas como confidenciais em todas as circunstâncias e serão utilizadas exclusivamente para propósitos de pesquisa, a menos que o entrevistado solicite ou concorde explicitamente com a divulgação a um terceiro.

Respeito ao entrevistado, expresso por um termo como: *“Ao obter sua cooperação, garantimos o respeito aos objetivos da pesquisa e asseguramos que as informações não serão utilizadas para outros fins”.*

Garantia de que a participação na pesquisa é voluntária. Isso pode ser expresso por um termo como: *“Em todas as formas de pesquisa sua cooperação é voluntária. Nenhuma informação pessoal será coletada de você ou sobre você sem seu prévio conhecimento e concordância”.*

Respeito à recusa, que pode ser expresso da seguinte forma: *“Você tem o direito de recusar a entrevista em qualquer estágio ou solicitar, posteriormente, que parte ou o todo de sua entrevista seja destruído ou excluído. Sempre que for possível, acataremos tal solicitação.”*

Tecnologias de identificação e rastreamento: informar claramente sobre quaisquer tecnologias e processamentos que estão sendo utilizados nessa pesquisa. Além de aplicativos específicos que podem ser descarregados para o computador ou equipamento do entrevistado, a maioria das pesquisas realizadas por meio da internet é capaz de detectar informações sobre o entrevistado sem seu conhecimento, tais como tipo de navegador, nome de usuário e IP. As informações devem ser claras quanto à captura, utilização e retenção destes dados durante a entrevista (exemplo: dados coletados para fins de rastreamento para que as páginas sejam adequadas ao navegador).

Cookies: informar claramente se cookies estão sendo utilizados e, caso estejam, por que. Exemplo: *“Utilizamos cookies e outros recursos semelhantes apenas para controle de qualidade, validação e para evitar a repetição incômoda da pesquisa”.* Caso cookies sejam utilizados, seria aconselhável incluir um lembrete informando que o entrevistado pode controlar se seu computador aceita cookies. Exemplo: *“Certifique-se de que seu navegador esteja configurado de forma que você seja alertado sobre a inserção de todos os cookies. Você também pode excluir cookies ajustando as configurações de seu navegador”.*

Crianças: informar claramente sobre como entrevistas com crianças serão conduzidas. Exemplo: *“Em pesquisas envolvendo crianças é necessário obter a permissão de um dos pais ou responsável legal pela criança antes do início da entrevista”.*

Como entrar em contato conosco: É necessário disponibilizar um endereço de correspondência, um endereço de e-mail e/ou um número de telefone não tarifado para que o entrevistado entre em contato com a empresa em caso de dúvidas ou outras necessidades.

Medidas de segurança. Exemplo: *“Nosso website possui medidas de segurança para evitar a utilização incorreta e alteração das informações que você nos fornecer. Apenas funcionários autorizados têm acesso às informações para propósitos de análise de dados e controle de qualidade. Caso dados pessoais sejam transferidos a terceiros, garantimos o mesmo nível de segurança”.*

E-mail não autorizado: divulgar a política sobre envio de e-mails não autorizados e repasse de endereços de e-mail a outros.

Acesso a informações pessoais: informar como acessar ou corrigir as informações retidas sobre um entrevistado.

Data da última atualização da política de privacidade.

B. Três elementos adicionais que precisarão ser incluídos, de acordo com as metodologias utilizadas para contatar entrevistados em potencial.

i. Quando o entrevistado estiver sendo **convidado a fazer parte de um painel** para propósitos de pesquisa de mercado, ou já fizer parte, é necessário:

- **Descrever** o processo de registro da inscrição.

- Descrever as informações que serão armazenadas na base de dados dos participantes da pesquisa para gestão de painel, controle e seleção de amostra, bem como o processo para atualizá-la.

- **Indicar a contrapartida que envolve a participação no painel, como frequência de participação em pesquisas, tempo máximo de participação, entre outros indicadores.**

- **Descrever o sistema de identificação com senha, caso haja,** e a segurança que oferece.

- **Explicar as políticas de inclusão e exclusão do painel para** manutenção ou programas de recompensas.

- Declarar quais comunicações serão enviadas e esclarecer quaisquer comunicações em potencial em nome de terceiros.

- **Explicar o funcionamento** do programa de recompensas

ii. Quando o pesquisador tiver obtido **uma lista de endereços de e-mail** para enviar convites para participação em uma pesquisa, é preciso ter atenção aos seguintes pontos:

- **Fonte das informações:** informar claramente a procedência do endereço de e-mail que será utilizado na pesquisa. Uma declaração do fornecedor da lista deve comprovar que os indivíduos listados estejam esperando um contato via e-mail.

- **Envio de spam:** pessoas que não consentiram em responder a pesquisa devem ter à disposição um mecanismo para remover seu nome de futuras pesquisas.

- **Sistema de identificação com senha:** se utilizado, descreva como funciona e a segurança que oferece.

- Processo de entrevista com **interrupção e reinício:** se este processo for possível, explique como funciona.

iii. Em **levantamentos de interceptação** nos quais o entrevistado é selecionado como uma amostra 1-em-n dos visitantes a um website, ou por meio de outra técnica semelhante:

- Explique a técnica de interceptação: ex., seleção aleatória.
- Descreva como funciona e a segurança que oferece o sistema de identificação por senha, quando for utilizado.
- Explique como funciona o processo de entrevista com interrupção e reinício, quando houver, e quais informações serão armazenadas para permiti-lo.
- Descreva qualquer processo invisível utilizado para efetuar a interceptação ou redirecionar os entrevistados para o levantamento.

Veja o Apêndice 2 – Exemplo de Política de Privacidade

2.4 Crianças e jovens/menores de idade

Pesquisadores devem ser sensíveis às preocupações de pais, grupos de consumidores e legisladores sobre a exploração em potencial de crianças e jovens/menores de idade na internet. Todas as medidas cabíveis devem ser tomadas para garantir que a permissão comprovada e explícita seja obtida de um dos pais ou guardião legal para convidar uma criança para participar de uma pesquisa, apesar de ser reconhecido que não é possível comprovar integralmente a identificação do respondente de pesquisa na internet, incluindo crianças e jovens/menores de idade.

2.4.1 Obtendo permissão

Pesquisadores devem observar todas as leis e códigos nacionais relevantes especificamente relacionados a crianças e jovens/menores de idade. As diretrizes da ESOMAR sobre entrevistas com crianças e jovens/menores de idade recomenda que indivíduos abaixo de 14 anos de idade sejam tratados como “crianças” e indivíduos entre 14 e 17 anos de idade, como “jovens/menores de idade”, pois a pesquisa de mercado está fundamentada nas ciências sociais e reconhece estágios de desenvolvimento mental e psicológico diferentes.

Antes de entrevistar crianças, pesquisadores devem certificar-se de que a permissão seja obtida junto a um dos pais, guardião legal ou outra pessoa legalmente responsável pela criança (doravante, ‘pai’).

Questionários em websites destinados a crianças devem exigir que a criança forneça sua idade antes de que quaisquer outras informações pessoais sejam solicitadas. Se a idade fornecida estiver abaixo da definição de criança acordada nacionalmente, a criança não deve ser convidada a fornecer informações pessoais adicionais até que a permissão apropriada seja obtida. Esta notificação deve ser clara e destacada, incluindo uma explicação do assunto e fazendo referência ao fato de que a permissão será verificada, quando necessário. A solicitação de permissão a um pai deve ser disponibilizada no website do fornecedor da pesquisa ou enviada por e-mail.

Quando as informações pessoais coletadas de crianças forem utilizadas exclusivamente para propósitos de pesquisa e nenhum dado pessoal for repassado para qualquer outro propósito, a permissão poderá ser um e-mail de resposta do pai ou outro método apropriado que esteja em conformidade com as leis e códigos nacionais relevantes.

Após solicitar à criança que forneça as informações de contato de seus pais para que a permissão possa ser obtida, medidas cabíveis devem ser tomadas para validar que os pais realmente concordaram através de um e-mail ou telefonema, por exemplo.

A permissão prévia dos pais não é exigida para:

- Coletar o endereço de e-mail da criança ou dos pais exclusivamente para notificar a coleta de dados e solicitar permissão.
- Coletar a idade da criança para propósitos de seleção e exclusão. Se tal seleção levar à decisão de que uma criança se qualifica para a entrevista, deve-se obter a permissão dos pais para prosseguir com a entrevista.

Deve-se evitar perguntas a crianças e jovens/menores de idade sobre tópicos geralmente considerados sensíveis, tais como sexo, drogas, álcool, violência, fumo, entre outros. Quando estes temas forem abordados, deve-se assegurar que os entrevistados não sejam afetados negativamente pela sua participação na pesquisa.

Informações pessoais relacionadas a outras pessoas (por exemplo, pais) devem ser coletadas com cautela junto às crianças.

No recrutamento de crianças para painéis, os pesquisadores devem considerar:

- O pesquisador deve recrutar pais com crianças da idade exigida e então administrar a pesquisa com a concordância e o acompanhamento da atividade pelo pai.
- Permitir a proteção por senha ou outra ferramenta que comprove a ciência do pai para que a criança prossiga com a pesquisa.

Quando necessário, pesquisadores deverão consultar a ABEP ou as Diretrizes ESOMAR para aconselhamento.

3. QUESTÕES REGULATÓRIAS

3.1 Dados pessoais e endereços de IP

Um endereço de IP, especialmente em conjunto com outros dados cadastrais, pode ser considerado um elemento de identificação do respondente em uma pesquisa. Portanto seu uso está sujeito a todas as normas referentes ao sigilo e identificação do respondente em pesquisa de mercado.

3.2 Jurisdição nacional

O [Código Internacional ICC/ESOMAR](#) deverá ser aplicado em justaposição às leis aplicáveis e quaisquer padrões ou regras mais rígidos que possam ser exigidos em qualquer mercado específico.

Em projetos internacionais, quando for possível saber o país de residência dos entrevistados, o pesquisador deverá seguir as exigências legais daquele país.

3.2.1 Coleta de dados à distância e transferência de dados

É recomendado aos pesquisadores que esclareçam, na política de privacidade, quais países deverão ser incluídos no projeto. O idioma do site ou questionário ajudará a esclarecer os países-alvos, que também deverão ser especificados na política de privacidade, que deverá obedecer as regulamentações de onde a empresa de pesquisa estiver estabelecida.

Para abordagens diferentes de painéis (inclusive interceptação na internet), a prática supracitada é mais apropriada. Entrevistados deverão ser informados das leis sob as quais os dados estão sendo coletados na página inicial da pesquisa, no ponto onde pede-se ao entrevistado que dê seu consentimento. Esse procedimento esclarecerá as condições quando o país de residência do entrevistado não for conhecido, como por exemplo, em pesquisas mundiais sobre satisfação dos clientes ou ao monitorar um site no qual os entrevistados poderiam estar localizados em qualquer lugar. Para painéis, a prática comum é informar os entrevistados sobre a lei em vigor através do registro no painel e das políticas de privacidade.

Antes que dados pessoais sejam transferidos do país de coleta a um terceiro país, o pesquisador deverá certificar-se de que a transferência de dados seja legal e que todas as medidas cabíveis sejam tomadas para garantir a segurança apropriada para preservar os direitos de proteção de dados dos indivíduos. Isso também se aplica se um servidor “remoto” estiver sendo utilizado em um país diferente para coletar dados do entrevistado, ou se os dados forem processados em uma “nuvem” internacional.

O pesquisador deverá explicar este processo em sua política de privacidade (veja o [conteúdo recomendado para políticas de privacidade](#) e o [exemplo de política de privacidade no Apêndice 2](#)) e oferecer as medidas de segurança apropriadas para proteger os dados pessoais ao solicitar a permissão do entrevistado para a transferência de dados.

3.3 Registro

Em países onde há legislação sobre proteção de dados, os controladores de dados normalmente são obrigados a registrar-se junto às autoridades.

3.4 Segurança

Pesquisadores e seus subcontratados devem tomar precauções apropriadas para oferecer o nível máximo de segurança ao coletar dados que possam ser identificados pessoalmente e, em particular, quaisquer dados confidenciais que possam estar definidos na legislação sobre proteção de dados como exigindo gestão particularmente cuidadosa (veja a [seção 6](#)).

Pesquisadores também devem tomar as medidas cabíveis para garantir que quaisquer informações confidenciais fornecidas a eles por clientes ou outros sejam protegidas contra acesso não autorizado. Exemplo: por *firewall* e controles de senha.

Clientes deverão ser plenamente informados e estar cientes sobre os riscos em potencial de postar detalhes de informações confidenciais em pesquisa na internet e deve ser exigido que implementem procedimentos de segurança rígidos. De forma geral, conceitos e ideias não podem ser protegidos apenas por meios tecnológicos e as declarações, uma vez distribuídas, ainda quando protegidas por acordos de confidencialidade, podem ser facilmente encaminhadas e efetivamente impossíveis de retirar de circulação uma vez que sejam divulgadas.

3.4.1 Gerenciando a segurança

Pesquisadores deverão utilizar tecnologias de segurança para proteger os dados pessoais coletados ou armazenados em websites ou servidores, utilizando sistemas de criptografia confiáveis, tais como o modo *Secure Socket Layer* (SSL), ou segurança de nível equivalente. Se a lei nacional relevante exigir, dados temporários também deverão ser criptografados a um nível apropriado.

A segurança de dados é importante para evitar acesso não autorizado, manipulação ou divulgação de dados que possam ser identificados pessoalmente, inclusive durante a transferência de dados. O fornecedor de pesquisa deverá ter políticas e procedimentos claros para gerir a segurança. O acesso aos dados deverá ser restrito e permitido exclusivamente com base na necessidade da informação. O pesquisador deve certificar-se de que todos os gerentes e pessoal-chave que tenham acesso a tais dados confidenciais tenham assinado acordos confirmando que seguirão o [Código ICC/ESOMAR](#) e não divulgarão dados pessoais.

Se a armazenagem temporária dos dados coletados ocorrer em um servidor que for operado por um subcontratado ou prestador de serviços, o pesquisador deverá colocar os subcontratados sob uma obrigação contratual para que tomem as precauções necessárias a fim de evitar acesso não autorizado enquanto os dados estiverem armazenados ou durante a transferência de dados. Os dados identificáveis retidos pelo prestador de serviços deverão ser excluídos o mais breve possível.

4. UTILIZANDO TECNOLOGIAS DE IDENTIFICAÇÃO E RASTREAMENTO ONLINE EM PESQUISAS

Tecnologias de identificação e rastreamento online se desenvolveram rapidamente nos últimos anos no âmbito global. Apesar de muitas dessas tecnologias terem sido desenvolvidas para aprimorar a experiência do usuário, causaram debates por parte de grupos de privacidade preocupados com o potencial, para organizações ou indivíduos, de identificar e monitorar indivíduos online sem seu conhecimento.

As tecnologias de identificação e rastreamento online desenvolvidas para pesquisa de mercado, de opinião e social são aplicadas para melhorar a integridade de painéis de pesquisa e técnicas de amostragem, já que o pesquisador e o participante irão interagir apenas online.

A ESOMAR, trabalhando em cooperação próxima ao CASRO (Conselho Americano de Organizações de Pesquisa) e à indústria global de pesquisa, estabeleceu orientações claras sobre a condução de pesquisa de mercado, social e de opinião utilizando tecnologias online e, ao fazê-lo, procura promover padrões profissionais, boas práticas e relacionamentos respeitosos com participantes de pesquisas.

4.1 Tecnologias de identificação e rastreamento para pesquisas

Tecnologias de identificação e rastreamento são tecnologias utilizadas para identificar, validar e rastrear entrevistados ou a atividade dos entrevistados para pesquisas via internet. O uso destas tecnologias pode incluir o rastreamento de propagandas, controle de quotas em levantamentos, prevenção de fraudes e pesquisa comportamental. Os termos *spyware* e *malware* são amplamente utilizados para descrever o uso inaceitável das tecnologias de rastreamento e identificação online. Pesquisas de mercado, sociais e de opinião não deverão utilizar tecnologias que podem ser classificadas como *spyware* ou *malware*. Esta seção estabelece os usos aceitáveis e inaceitáveis desta tecnologia, assim como fornece orientações sobre tipos de tecnologia específicos.

4.1.1 Tecnologias específicas

Tecnologias de identificação e rastreamento para pesquisas incluem:

Cookies

Pequenos arquivos de texto armazenados em um computador por um website que atribui um ID de usuário numérico e armazena determinadas informações sobre sua navegação online. *Cookies* são utilizados em websites de pesquisas para ajudar o pesquisador a reconhecer o entrevistado como um usuário que já respondeu a pesquisa, assim como para outras funções de controle da qualidade da pesquisa. Os dados armazenados em *cookies* não são personalizados e podem ser rejeitados ou excluídos por meio das configurações do navegador.

Pesquisadores deverão incluir informações claras, concisas e destacadas sobre a utilização de *cookies* em suas pesquisas e as razões para essa prática. Veja a seção de diretrizes [sobre políticas de privacidade](#). Se *cookies* forem utilizados, o pesquisador deverá certificar-se de que a descrição dos dados coletados e seus usos sejam plenamente divulgados na política de privacidade da organização de pesquisa.

Pesquisadores coletando dados de painéis e rastreando o comportamento dos entrevistados na internet precisam incluir tais atividades em sua declaração de privacidade (veja a seção sobre [dados de painéis](#)) e também deverão explicar esta atividade na página de inscrição no painel, para garantir que entrevistados estejam completamente esclarecidos sobre as informações que serão coletadas.

Flash cookies

Originam-se da codificação encontrada no *Flash Media Player* da empresa Adobe, um aplicativo que é utilizado pela maioria dos websites comerciais que incluem animações ou vídeos.

Se utilizado em uma técnica de pesquisa, os pesquisadores devem divulgar o uso destas informações, fornecer detalhes sobre como removê-los em sua política de privacidade (veja a seção de diretrizes [sobre políticas de privacidade](#)) e obter prévio consentimento dos entrevistados. Esta regra aplica-se também a novas tecnologias que executem a mesma função.

ID do aparelho (também chamada de *digital fingerprinting* ou ID de máquina)

Estas são tecnologias que, por meio de um algoritmo, analisam um grande número de características e configurações técnicas para gerar um identificador exclusivo, capaz de identificar um computador específico, gerando uma ID do aparelho ou uma ID de máquina.

Tecnologias de agente ativo

São aplicativos ou aparelhos que capturam o comportamento do entrevistado em segundo plano, tipicamente quando são executados de forma concomitante a outras atividades. Incluem:

- Aplicativo descarregado direto na área de trabalho do computador do usuário, que é utilizado exclusivamente com o propósito de alertar entrevistados em potencial sobre os levantamentos, descarregando o conteúdo ou respondendo a perguntas. O aplicativo não rastreia os sujeitos dos dados à medida que navegam pela internet e todos os dados coletados são fornecidos diretamente através da entrada de dados pelo usuário;
- Aplicativo de rastreamento que pode capturar o comportamento online real do sujeito dos dados, tais como acessos a páginas em websites, páginas visitadas, transações online concluídas, formulários online preenchidos, taxas de clique ou impressão de anúncios e compras online. Esse aplicativo também tem a capacidade de capturar informações do e-mail do sujeito dos dados e de outros documentos armazenados em um aparelho, tal como um disco rígido. Parte desta tecnologia foi rotulada “*spyware*,” particularmente se o descarregamento ou instalação do aplicativo ocorrer sem pleno conhecimento e consentimento do sujeito dos dados.

O uso de *spyware* por pesquisadores é estritamente proibido.

4.1.2 Declaração sobre tecnologias de identificação e rastreamento

As informações relacionadas ao uso de tecnologias de identificação e rastreamento devem ser transparentes e efetuadas antes ou no momento da coleta. Para projetos individuais, tais declarações podem fazer parte do convite de recrutamento e uma política de privacidade específica ao projeto deve ser aplicada. Se uma tecnologia em particular for utilizada em diversos ou todos os projetos, as declarações relacionadas à tecnologia devem fazer parte da política de privacidade geral da organização de pesquisa para entrevistados online. Atalhos a políticas de privacidade específicas do projeto e/ou gerais deverão estar facilmente acessíveis aos entrevistados (por exemplo: nos convites para pesquisa e/ou na página inicial de pesquisa online).

Exemplos são fornecidos no Apêndice 2 para o uso de:

[Cookies](#)

[Flash cookies](#)

[Cookies e aplicativos para rastreamento](#)

[Identificação de aparelhos/máquinas](#)

4.2 Práticas que organizações de pesquisa devem adotar

A seguir uma lista de práticas que pesquisadores que utilizam tecnologias de identificação e rastreamento deverão adotar. Pesquisadores que adotarem estas práticas e evitarem o exposto no tópico 4.3 não serão considerados usuários de *spyware*.

Transparência é fundamental. Pesquisadores devem divulgar informações sobre tecnologias de identificação e rastreamento e outros aplicativos de forma oportuna e aberta aos entrevistados. Esta comunicação deverá fornecer detalhes sobre como o pesquisador utiliza e compartilha as informações dos entrevistados.

- Apenas após receber a permissão do entrevistado (permissão do pai ou guardião legal, no caso de crianças) qualquer aplicativo de pesquisa poderá ser descarregado para o computador ou aparelhos do indivíduo.¹
- Pesquisadores deverão comunicar claramente ao entrevistado os tipos de dados, se houver, que estão sendo coletados e armazenados por uma tecnologia de identificação e rastreamento em particular.
- Também é necessária declaração para permitir ao entrevistado que desinstale facilmente o aplicativo de pesquisa sem prejuízo ou dano a ele ou ao seu equipamento.
- Informações pessoais sobre o entrevistado não deverão ser utilizadas para propósitos secundários ou compartilhadas com terceiros sem o consentimento do entrevistado.

¹ Esta exigência e muitas das outras nesta seção não se aplicam a computadores ou equipamentos de captura de dados fornecidos ao entrevistado pelo pesquisador, pois nestes casos o pesquisador continua sendo o proprietário e controlador do aparelho.

- v. Pesquisadores devem certificar-se de que a participação na pesquisa seja uma atividade consciente e voluntária. Portanto, incentivos nunca deverão ser utilizados para ocultar ou ofuscar o aceite de tecnologias de identificação e rastreamento para pesquisas.
- vi. Pesquisadores devem certificar-se de que haja um canal para receber dúvidas dos entrevistados.
- vii. De forma rotineira e contínua, consistente com as políticas divulgadas pela empresa de pesquisa, os entrevistados que participarem do painel de pesquisas deverão receber notificações claras e periódicas esclarecendo que eles estão registrados ativamente como participantes, para assegurar que sua participação seja voluntária. Pesquisadores deverão fornecer aos entrevistados que participam de um painel de pesquisas um método claramente definido para desinstalar o aplicativo de rastreamento do pesquisador sem causar danos ao sujeito dos dados.
- viii. Ao instalar atualizações a aplicativos para corrigir erros, problemas de segurança ou novas versões que não modifiquem o escopo dos dados pessoais que são coletados, se não houver resposta à notificação após um período de tempo aceitável (30 dias), pode ser presumido que o participante concordou. Esta suposição deverá ser incluída na declaração de privacidade. Se o pesquisador decidir reduzir o período de notificação de 30 dias para um aplicativo específico, deverá ser explicitamente mencionado em um lugar visível no website.

A manipulação responsável dos dados é fundamental. Pesquisadores deverão tomar medidas para proteger as informações coletadas dos entrevistados.

- i. Dados pessoais ou confidenciais não deverão ser coletados a menos que haja consentimento da pessoa pesquisada. Se o consentimento não for obtido e a coleta for inevitável, os dados deverão ser destruídos imediatamente. Se esse procedimento não for possível, os dados deverão receber o nível máximo de segurança de dados e não deverão ser acessados ou utilizados para qualquer outro propósito.
- ii. Pesquisadores deverão estabelecer medidas de segurança que minimizem os riscos e as ameaças à privacidade para os entrevistados.
- iii. É importante que pesquisadores entendam o impacto de sua tecnologia para os entrevistados, particularmente quando seu aplicativo for descarregado em um pacote com outros aplicativos.
- iv. Pesquisadores devem fazer todos os esforços cabíveis para garantir que estes aplicativos (quer sejam livres de custos ou não) sejam inofensivos, seguros e não ofereçam riscos indevidos à privacidade ou segurança dos dados dos painelistas.
- v. Pesquisadores também deverão ser proativos na gestão da rede de participantes do painel, monitorando e tomando providências em relação a eventos incomuns, tal como abandono.

4.3 Práticas inaceitáveis

A seguir encontra-se uma lista de práticas inaceitáveis, estritamente proibidas aos pesquisadores. Será considerado que pesquisadores estão utilizando *spyware* quando não adotarem qualquer uma das práticas estabelecidas abaixo:

- i. Descarregar aplicativos sem obter consentimento do entrevistado;
- ii. Descarregar aplicativos sem fornecer plena notificação e declaração sobre os tipos de informações que serão coletadas sobre o entrevistado e como estas informações poderão ser utilizadas pelo pesquisador. Tal notificação deverá ser clara, concisa e destacada;
- iii. Coletar informações que identifiquem o entrevistado sem obter consentimento;
- iv. Utilizar registradores de teclado (*keystroke loggers*) sem obter o consentimento de inclusão do entrevistado (opt-in);
- v. Instalar aplicativos que modifiquem as configurações do computador do entrevistado além do necessário para conduzir pesquisas;
- vi. Instalar aplicativos que desabilitem aplicativos anti-*spyware*, antivírus, ou anti-*spam* ou que assumam o controle do aparelho do entrevistado;
- vii. Ausência de todos os esforços cabíveis para certificar-se de que o aplicativo não cause quaisquer conflitos com os principais sistemas operacionais;
- viii. Instalar aplicativos que estejam ocultos dentro de outros aplicativos que possam ser descarregados ou difíceis de desinstalar;
- ix. Instalar aplicativos que forneçam conteúdo publicitário, com exceção de aplicativos para o propósito de testes publicitários;
- x. Instalar atualizações a aplicativos sem notificar usuários e dar ao participante a oportunidade de recusar tais atualizações;

- xi. Alterar a natureza das tecnologias de identificação e rastreamento sem notificar o usuário;
- xii. Não notificar o usuário sobre alterações à prática de privacidade relacionadas a atualizações de aplicativos;
- xiii. Rastrear o conteúdo do e-mail do entrevistado;
- xiv. Se o navegador do entrevistado estiver configurado em modo privado, o pesquisador não deverá rastrear o comportamento a menos que seja obtido consentimento de inclusão do entrevistado (opt-in);
- xv. Quando o entrevistado estiver em um website configurado para conexão segura (ou seja, um website SSL), o pesquisador não deverá coletar dados pessoais, a menos que seja obtido consentimento de inclusão do entrevistado (opt-in);

4.4 Aparelhos interativos de telefonia móvel e *smartphones*

Aparelhos interativos de telefonia móvel e *smartphones* são capazes de combinar as características de um aparelho de telefonia móvel e um navegador de internet. A ESOMAR publicou diretrizes sobre pesquisas online (este documento) e sobre [pesquisas utilizando aparelhos de telefonia móvel](#). As diretrizes apropriadas a seguir para aparelhos interativos de telefonia móvel dependem se o pesquisador contata o entrevistado utilizando os recursos de um aparelho de telefonia móvel (ou seja, fazendo uma ligação ou enviando mensagens de texto – *SMS*) ou utilizando os recursos de internet (ou seja, e-mail, atalho no navegador de internet ou aplicativo baixado). Se uma combinação dos dois métodos for utilizada, como por exemplo, aparelho de telefonia móvel para contatar e navegador de internet para responder, as partes apropriadas das duas diretrizes deverão ser aplicadas.

4.4.1 Utilizando aparelhos interativos de telefonia móvel

Contatando

Ao utilizar metodologias online para contatar pessoas, pesquisadores só deverão conduzir abordagens autorizadas por e-mail e/ou outras mensagens (ex., mensagens instantâneas, *SMS*, etc.) para entrevistados em potencial. Pesquisadores são obrigados a verificar se os indivíduos contatados por tais meios para pesquisas autorizam o contato para pesquisas. Veja a [seção 2.2](#) sobre notificações e e-mail.

Segurança e download de aplicativos

Quando pesquisadores instalarem aplicativos (*apps*) em aparelhos interativos de telefonia móvel, deverão seguir as [seções 4.1.1 e 4.1.2](#) dessas diretrizes. Pesquisadores deverão dar acesso aos entrevistados às suas políticas de privacidade. Além de seguir a [seção 3.4](#), pesquisadores deverão certificar-se de que quaisquer dados armazenados localmente no aparelho estejam seguros e indisponíveis para outras pessoas, caso o aparelho seja furtado ou utilizado por outra pessoa. Esse processo pode ser garantido por meio da encriptação dos dados.

Custo para o entrevistado

Entrevistados utilizando aparelhos interativos de telefonia móvel para participarem de pesquisas poderão incorrer em custos de minutos de conexão, roaming ou transmissão de dados. Se possível, o pesquisador deverá planejar o estudo para que o entrevistado não incorra em custos. Se não for possível, o pesquisador deverá estar preparado para restituir os entrevistados por seus custos. Quando os aparelhos de telefonia móvel interativos dos entrevistados são adicionados a um painel ou base de dados de amostragem, a questão de custos e restituição deverá ser acordada no estágio da “inscrição”.

Configuração apropriada

Ao contatar entrevistados que estão utilizando aparelhos interativos de telefonia móvel, o pesquisador deverá certificar-se de que a configuração da pesquisa seja apresentada em um formato apropriado, otimizada para diversos aparelhos, como provavelmente será visualizada pelos participantes. Os entrevistados também deverão ter a oportunidade de optar por não participar da pesquisa em questão.

Política de privacidade

Devido a limitações de espaço das telas de aparelhos interativos de telefonia móvel, pode ser difícil exibir uma política de privacidade integral. Pesquisadores deverão aplicar uma solução apropriada e tomar as medidas adequadas para minimizar os custos e maximizar a praticidade para acessar as informações relevantes. Por exemplo, pesquisadores deverão fornecer um atalho de internet para sua política de privacidade, com a menor URL possível, e oferecer um número de telefone não tarifado e/ou um endereço de correspondência.

Dados de localização e GPS

Agora é possível capturar dados adicionais de aparelhos interativos de telefonia móvel e *smartphones*, tais como dados de localização em tempo real. As diretrizes da ESOMAR sobre [Passive Data Collection](#) tratam deste assunto. O pesquisador deverá obter a permissão do entrevistado antes de capturar tais dados.

5. QUESTÕES METODOLÓGICAS

5.1 Amostras online

Há diversas formas para recrutar amostras online e estas exigem formulários de consentimento diferentes (veja a [seção 2.3](#) sobre políticas de privacidade). Os dados pessoais dos integrantes de um painel são retidos pelo fornecedor do painel, enquanto outras formas de amostragem não exigem normalmente que os dados pessoais sejam retidos pelo prestador de serviços de pesquisas. Para armazenar os dados pessoais dos indivíduos, deve-se ter consentimento apropriado antes ou no momento da coleta.

5.2 Painéis de acesso

As diretrizes que regulamentam os painéis de acesso estão descritas nas 26 perguntas da ESOMAR, que podem ser encontradas no Apêndice 3 da edição original dos Códigos e Diretrizes da ESOMAR.

5.3 Detalhes técnicos

O [Código ICC/ESOMAR](#) sobre conduta (Artigos 4d e e) exige que os pesquisadores forneçam detalhes técnicos completos sobre a metodologia de pesquisa utilizada ao conduzir um projeto; pesquisas online também poderão ter metodologias e estratégias de amostragem complexas. Isso torna ainda mais importante que os detalhes técnicos sejam reportados de tal forma a tornar possível a reprodução do estudo.

As Diretrizes ESOMAR Sobre os [Direitos e Responsabilidades Mútuos](#) de Pesquisadores e Clientes estabelece as exigências para o reporte técnico de projetos de pesquisa de acordo com o [Código ICC/ESOMAR](#). Essas diretrizes aplicam-se a todos os projetos de pesquisa, incluindo pesquisas online.

6. DEFINIÇÕES E FONTES DE INFORMAÇÕES ÚTEIS

Para os propósitos destas diretrizes, três conceitos-chave (pesquisador, dados pessoais e consentimento) são tratados abaixo:

Pesquisador: definido no [Código Internacional ICC/ESOMAR](#) como qualquer indivíduo ou organização executando ou atuando como um consultor em um projeto de pesquisa de mercado, inclusive indivíduos trabalhando nas organizações-clientes.

Dados pessoais compreendem quaisquer informações relacionadas a uma pessoa física identificada ou identificável, ou seja, um indivíduo privado, em oposição a uma pessoa jurídica ou outra entidade comparável. Uma pessoa identificável é alguém que pode ser identificado direta ou indiretamente através de um número de identificação ou de características físicas, fisiológicas, mentais, econômicas, culturais ou sociais.

Dados pessoais confidenciais compreendem quaisquer informações sobre a origem racial ou étnica, saúde ou vida sexual, registros criminais, opiniões políticas, crenças religiosas ou filosóficas ou associação a sindicatos trabalhistas de um indivíduo identificável. As informações pessoais relacionadas à saúde, renda ou outras informações financeiras e documentos de identidade ou financeiros emitidos pelo governo também são considerados confidenciais.

Consentimento significa o acordo dado de forma livre e informado por um indivíduo para a coleta e processamento de seus dados pessoais. Em pesquisa de mercado, esse consentimento está baseado no fato de que o entrevistado fornece voluntariamente as respostas em uma pesquisa após receber informações claras sobre a natureza dos dados sendo coletados, o propósito para o qual serão utilizados e a identidade da pessoa ou organização retendo os dados pessoais. O entrevistado pode retirar seu consentimento a qualquer momento, recusando-se a cooperar em uma entrevista ou projeto de pesquisa.

Legislação-chave relevante

Leis de proteção de dados são específicas para cada setor já que, atualmente, não existe uma única lei nacional abrangente sobre privacidade que se aplique a todas as organizações no setor privado. Sendo assim, o que vale é o código civil brasileiro.

Observação

Os itens relativos a outros países, que não o Brasil, foram excluídos do texto original da ESOMAR.

Fontes úteis

As fontes a seguir oferecem materiais úteis e relevantes para o pesquisador online:

ACE *Association Collaborative Effort*: Um conjunto de definições atualizadas para conceitos-chave de pesquisas pela internet foi desenvolvido aqui;

AMSRO Código de Privacidade em Pesquisa de Mercado e Pesquisa Social e Princípios de Privacidade em Pesquisa Social;

COPPA Lei de Proteção à Privacidade Online das Crianças;

CASRO Código de Padrões e Ética para Pesquisas de Levantamentos, Seção 3. Pesquisa pela internet;

ADM Declaração para o Território da República Federal da Alemanha em relação ao Código Internacional ICC/ESOMAR sobre Pesquisa de Mercado e Pesquisa Social e orientações;

DMA Código de Prática para Comunicações Comerciais Online para Crianças;

Diretrizes **para Levantamentos Online** (Alemanha), subscrito por ADM, ASI, BVM, DGOF;

MRS Código e Diretrizes para Pesquisas com Crianças e Jovens/Menores de Idade;

U.S.-EU & Swiss Safe Harbour Frameworks: Com o intuito de aproximar as diferentes abordagens de privacidade dos EUA e da UE e oferecer um meio simplificado para organizações estadunidenses obedecerem à Diretiva da UE ao transferir dados pessoais da UE aos EUA, o Departamento de Comércio dos EUA, em consultoria com a Comissão Europeia, desenvolveu uma estrutura *Safe Harbour* para fornecer as informações que uma organização precisaria para avaliar e então ingressar no código *Safe Harbour*;

Comissão Europeia: Modelos de contratos para a transferência de dados pessoais da UE;

ISO 26362:2009: Comunicado à imprensa sobre painéis de acesso em pesquisas de mercado e pesquisas de opinião – Vocabulário e exigências de serviço;

ISO 20252:2006: Pesquisa de mercado, pesquisa de opinião e pesquisa social – Vocabulários e exigências de serviço.

Diretrizes adicionais

ABEP – Associação Brasileira das Empresas de Pesquisa (www.abep.org)

APÊNDICE 1 – Princípios-chave do Código ICC/ESOMAR

1. Pesquisadores de mercado deverão obedecer a todas as leis nacionais e internacionais.
2. Pesquisadores de mercado deverão comportar-se de maneira ética e não deverão agir de forma a prejudicar a reputação da atividade de pesquisa de mercado.
3. Pesquisadores de mercado deverão tomar cuidados especiais ao executar pesquisas envolvendo crianças e jovens/menores de idade.
4. A colaboração dos entrevistados é voluntária e deve basear-se em informações adequadas – e não enganosas – sobre o propósito e natureza geral do projeto no momento que sua concordância em participar estiver sendo obtida. Todas as declarações então feitas deverão ser honradas.
5. Os direitos dos entrevistados como indivíduos privados deverão ser respeitados pelos pesquisadores de mercado e eles não deverão ser prejudicados ou afetados adversamente em resultado direto de sua cooperação em um projeto de pesquisa de mercado.
6. Pesquisadores de mercado nunca deverão permitir que qualquer informação pessoal coletada em um projeto de pesquisa de mercado seja utilizada para propósitos que não sejam pesquisa de mercado.
7. Pesquisadores de mercado deverão assegurar que projetos e atividades sejam planejados, executados, reportados e documentados de forma precisa, transparente e objetiva.
8. Pesquisadores de mercado deverão seguir os princípios aceitos de justa concorrência.

APÊNDICE 2 – Exemplo de Política de Privacidade

O exemplo fornecido abaixo oferece uma estrutura para uma política de privacidade. O texto não deverá ser tratado como completo ou atualizado em relação a todas as leis nacionais ou exigências locais. É responsabilidade do pesquisador certificar-se de que sua política satisfaça as exigências nacionais vigentes nos países nos quais estão operando.

A política está dividida em três seções principais: uma declaração concisa no primeiro nível sobre como a privacidade será protegida e os dados serão utilizados, uma introdução geral no segundo nível, que descreve o propósito e os princípios gerais e, no terceiro nível, uma seção detalhada cobrindo todos os aspectos de como o pesquisador trata dados pessoais.

EXEMPLO:

Nível 1

Obrigado por participar de nosso projeto de pesquisa.

1. Prometemos proteger sua privacidade e tratar as informações que nos fornecer como confidenciais.
2. As informações que você fornecer serão utilizadas exclusivamente para propósitos de pesquisa.
3. Não divulgaremos suas informações pessoais para terceiros sem seu consentimento.
4. Nunca tentaremos vender nada para você e nunca venderemos seus dados pessoais a qualquer pessoa. Este não é o nosso negócio. Não fazemos telemarketing ou marketing direto. Somos pesquisadores de mercado interessados exclusivamente em suas opiniões e comportamento.
5. Suas decisões sobre participar de um estudo, responder perguntas específicas ou interromper sua participação serão respeitadas sem questionamentos.

[Clique aqui para mais informações sobre pesquisa de mercado \(Nível 2\)](#)

[Clique aqui para nossa declaração de política de privacidade completa \(Nível 3\)](#)

Nível 2

Sua privacidade é importante para nós

Pesquisas de mercado, mídia e opinião exercem um papel importante na sociedade. Empresas e governos tomam decisões melhores com base em pesquisas de mercado. Como participante em uma pesquisa, suas opiniões ajudam empresas a desenvolver produtos novos, aprimorar produtos existentes e melhorar o atendimento ao cliente. Organizações políticas e governos também dependem de pesquisas de mercado para levar à frente as leis e políticas que o público precisa ou deseja.

Ao participar de uma pesquisa conduzida por nossa empresa, você pode estar certo(a) de que protegeremos sua privacidade. Ocasionalmente poderemos recontatá-lo(a) para validar suas respostas. Nunca deturparemos quem somos, suas respostas ou o que estamos fazendo.

Desenvolvemos padrões de privacidade rigorosos que estão estabelecidos em nossa política de privacidade detalhada. Nossa empresa é associada à ABEP (Associação Brasileira das Empresas de Pesquisa) e segue os padrões de ética que protegem a sua privacidade estabelecidos pela ESOMAR, a organização mundial para a promoção de boas práticas em pesquisas sobre mercados, consumidores e sociedades.

Caso tenha quaisquer perguntas ou preocupações relacionadas à privacidade, por favor entre em contato por e-mail (*inserir um endereço de e-mail*), por telefone (*inserir número de telefone não tarifado*), ou ainda enviando uma correspondência para nosso endereço (*inserir endereço de correspondência*).

Nível 3

Política de Privacidade

Data da criação: (*inserir data*)

Data da última revisão: (*inserir data*)

Nota aos pesquisadores: é uma boa prática incluir a data da última revisão para que os consumidores sejam informados quando as empresas efetuarem alterações substanciais a suas declarações de privacidade.

1. As informações que coletamos

Quando nossa empresa conduz pesquisas online, nossos convites e questionários nos identificam claramente e explicam os propósitos de nosso contato.

Quando o(a) contatamos, geralmente o fazemos por um dos propósitos a seguir:

- a. Convidá-lo(a) a participar de uma pesquisa;
- b. Realizar uma entrevista com você;
- c. Validar respostas que você forneceu em uma pesquisa que conduzimos;
- d. Atualizar e garantir que nossos registros de suas informações pessoais estejam corretos (apenas aplicável a painéis).

Ocasionalmente, podemos contatá-lo(a) por um destes outros propósitos:

1. Notificá-lo(a) se foi ganhador(a) em um sorteio de prêmios que patrocinamos;
2. Solicitar sua permissão para utilizar suas informações pessoais para um propósito que não lhe foi explicado na primeira vez que coletamos suas informações pessoais.

Ao participar de nossa pesquisa, podemos solicitar que forneça suas opiniões assim como informações demográficas, tais como sua idade e composição domiciliar. Você poderá recusar-se a responder determinadas perguntas ou interromper sua participação em uma pesquisa a qualquer momento. Se você ingressou em nosso painel de pesquisas pela internet, você poderá rescindir sua associação a qualquer momento seguindo as instruções para exclusão que incluímos em todos os e-mails que enviamos.

Nunca convidamos crianças abaixo de 14 anos para participarem de pesquisas sem tomar medidas para garantir o consentimento apropriado de seus pais.

2. Confidencialidade das respostas da entrevista e informações de contato

Combinamos suas respostas a uma pesquisa com as respostas de todos os outros que participaram e reportamos tais respostas de forma agregada ao cliente que encomendou a pesquisa. Não reportaremos intencionalmente suas respostas individuais, exceto conforme descrito abaixo.

Suas respostas às pesquisas poderão ser coletadas, armazenadas ou processadas por nossas empresas afiliadas ou por prestadores de serviços não afiliados, tanto dentro quanto fora do Brasil. Estas empresas estão obrigadas contratualmente a manter quaisquer informações que colem e divulguem para nós, ou que nós colemos e divulguemos para elas, em confidencialidade e devem protegê-las com padrões e práticas de segurança que sejam equivalentes aos utilizados para nossas próprias informações.

Além de manter suas respostas em confidencialidade, nunca venderemos, compartilharemos, alugaremos ou transferiremos intencionalmente seu nome, endereço, número de telefone ou endereço de e-mail para nossos clientes, outras empresas de pesquisa de mercado, empresas de marketing direto ou qualquer outra pessoa.

As únicas exceções nas quais poderemos divulgar suas informações pessoais ou respostas a pesquisas a terceiros são as seguintes:

1. Se você solicitar ou consentir que compartilhem suas informações de identificação e respostas individuais com terceiros para um propósito específico;
2. Segundo as diretrizes da ESOMAR, fornecemos suas respostas a um terceiro que esteja obrigado contratualmente a manter as informações divulgadas em confidencialidade e utilizá-las exclusivamente para propósitos de pesquisa;
3. Na rara, porém possível, circunstância que as informações estejam sujeitas à divulgação segundo intimações, mandados, ordens judiciais, governamentais, exigências legais ou regulatórias semelhantes.

3. Uso de *cookies*, arquivos de registros e outras tecnologias em nosso website

Cookies são pequenos arquivos de texto armazenados em seu computador por um website que atribui um identificador (ID) de usuário numérico e armazena determinadas informações sobre sua navegação online. Utilizamos *cookies* em nosso website de pesquisa para nos ajudar a oferecer-lhe uma melhor experiência e para outras funções de controle de qualidade e validação. Nenhuma informação pessoal é armazenada em qualquer *cookie* que utilizamos.

(Pode ser aplicável a painéis) Alguns dos *cookies* que utilizamos neste website são obrigatórios porque o(a) identificam como membro válido de nosso painel e protegem o acesso a seu perfil e às informações de sua conta. As configurações de privacidade de seu navegador deverão estar ajustadas para permitir *cookies* de (inserir URL do website), ou você não conseguirá registrar-se no painel (inserir URL do website) ou acessar a área de participantes deste website. Se desejar, você pode ajustar as configurações de privacidade de seu navegador para excluir *cookies* ao sair de websites ou ao encerrar seu navegador.

Este website utiliza *Flash Local Shared Objects* (LSO), também conhecidos como “*Flash cookies*,” para armazenar algumas de suas preferências, exibir conteúdo com base no que você visualiza, personalizar sua visita, combater fraudes que colocam em risco a qualidade da pesquisa, ou rastrear seu comportamento e atividades ao longo de diversas visitas ao website. Utilizamos *Flash cookies* estrita e exclusivamente para propósitos de pesquisa.

Flash cookies são diferentes de *cookies* de navegadores devido à quantidade e tipo de dados armazenados e à forma na qual os dados são armazenados. As versões mais recentes dos navegadores conhecidos agora permitem aos internautas que gerenciem *Flash cookies* utilizando as configurações de privacidade do navegador ou baixando complementos (*add-ons*).

Se seu navegador não suportar estas funções, você poderá gerenciar as configurações de privacidade e armazenagem para *Flash cookies* ou desabilitar seu uso completamente acessando o website da Macromedia, a fabricante do *Flash Player*, pelo seguinte atalho:

Adobe – Flash Player: Gerenciador de configurações:

http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager.html

(Aplicável à pesquisa de rastreamento comportamental) Utilizamos *cookies* opcionais, tanto baseados no navegador quanto em tecnologia Flash, (inserir “aplicativos” se isto aplicar-se a seu painel) para conduzirmos pesquisa sobre propagandas e websites. Estes *cookies* estão disponíveis apenas para os participantes de nosso painel que concordaram explicitamente em participar de nosso programa de pesquisa de rastreamento comportamental. Os *cookies* rastreiam determinadas propagandas online e páginas na internet que você visualiza, incluindo a frequência na qual o conteúdo online que estamos mensurando é exibido por seu computador. Apenas um pequeno número de propagandas ou websites são mensurados através deste programa de pesquisa e as informações que coletamos são utilizadas estritamente para propósitos de pesquisa. Nenhuma mensagem ou comunicação comercial será direcionada a você como resultado de sua participação nesta pesquisa. Detalhes completos sobre este programa estão disponíveis quando você estiver conectado(a) a nosso website, inclusive instruções sobre como interromper sua participação a qualquer momento.

Como a maioria dos websites, coletamos determinadas informações automaticamente e as armazenamos em arquivos. Estas informações incluem endereços de IP (Protocolo de Internet), tipo de navegador, prestador de serviços de internet (ISP), páginas de referência/saída, sistema operacional, registro de data/horário e dados sobre os atalhos clicados (*clickstream*). Utilizamos estas informações para analisar tendências, administrar nosso website, rastrear as movimentações dos usuários em nosso website e coletar informações demográficas sobre nossa base de usuários. Para nos proteger contra fraude, podemos associar estes dados coletados automaticamente às informações enviadas pelo endereço (inserir URL da empresa de pesquisas).

(Aplicável a IDs de aparelhos) Tecnologias de identificação de aparelhos atribuem um identificador exclusivo ao computador de um usuário para identificar e rastrear o computador. *(inserir o nome da empresa)* não utiliza tecnologia de identificação de aparelhos (também conhecida como ID de máquina ou *digital fingerprinting*) para coletar informações pessoais ou rastrear as atividades online de usuários de computadores. Utilizamos a tecnologia para ajudar nossos clientes a garantir a integridade dos resultados de pesquisas. A tecnologia analisa as informações e dados obtidos do navegador de internet de seu computador e, a partir de outros pontos de dados disponíveis publicamente – que incluem, por exemplo, as configurações técnicas de seu computador, características de seu computador e endereço de IP. Estes dados são utilizados para criar um identificador exclusivo atribuído a seu computador. Este identificador é uma ID alfanumérica que retemos, mas não retemos as informações analisadas pela tecnologia para criar este identificador. A tecnologia não interrompe ou interfere no uso ou controle de seu computador e não altera, ou modifica as configurações ou funcionalidades de seu computador.

Como apoio a nossos esforços para auxiliar nossos clientes a proteger e garantir a integridade dos resultados de pesquisas, nós:

- a. poderemos relacionar ou associar seu identificador exclusivo a você e a quaisquer das informações que você nos forneça;
- b. poderemos compartilhar seu identificador exclusivo com nossos clientes e com outros fornecedores de amostras ou painéis; e
- c. poderemos receber ou obter um identificador exclusivo associado a você por um terceiro, incluindo, sem limitações, um fornecedor de amostras ou painéis ou um cliente de nossa empresa.

Quaiquer identificadores exclusivos associados a um indivíduo específico serão protegidos segundo esta política de privacidade. Utilizaremos e compartilharemos a tecnologia de maneira profissional e ética segundo: nossa política de privacidade; quaisquer declarações e/ou divulgações feitas por nossa empresa a você; leis aplicáveis; códigos da indústria.

Na possibilidade de descobirmos ou ficarmos cientes sobre qualquer conduta não ética relacionada ao uso da tecnologia, ou que a tecnologia está sendo utilizada de uma forma que seja inconsistente com as declarações e/ou divulgações feitas por nós aos entrevistados ou em violação às leis e códigos aplicáveis, tomaremos ação imediata para proibir tal conduta não ética e para garantir a administração apropriada da tecnologia.

4. Segurança das informações pessoais

Informamos nossos funcionários sobre nossas políticas e procedimentos em relação à confidencialidade, segurança e privacidade e enfatizamos a importância da conformidade a eles. Nossos procedimentos de segurança são consistentes com os padrões comerciais geralmente aceitos utilizados para proteger informações pessoais.

Podemos transferir informações pessoais a empresas afiliadas ou a prestadores de serviços não afiliados para propósitos relacionados a pesquisas, tais como processamento de dados e realização de sorteios de prêmios ou outros incentivos. Exigimos destas empresas que protejam todas as informações pessoais de uma maneira que seja consistente com as medidas de nossa empresa e conforme regulamentado pela lei. Seguimos os padrões geralmente aceitos pela indústria para proteger as informações pessoais que nos são enviadas, tanto durante a transmissão quanto uma vez que as tenhamos recebido.

5. Precisão das informações pessoais

(inserir nome da empresa) faz todos os esforços cabíveis para manter as informações pessoais sob controle, que são utilizadas continuamente, precisas, completas, atualizadas e relevantes, com base nas informações mais recentes que são disponibilizadas. Dependemos de você para nos ajudar a manter suas informações pessoais precisas, completas e atualizadas, respondendo nossas perguntas honestamente.

6. Acesso a informações pessoais

Para solicitar acesso às informações pessoais que retemos a seu respeito, pedimos que envie sua solicitação por escrito ao endereço de e-mail ou endereço de correspondência exibidos abaixo (na seção Como entrar em contato conosco). Você poderá acessar suas informações pessoais e corrigir, alterar ou excluir o que estiver incorreto.

Nós iremos nos esforçar para fornecer a você as informações pessoais solicitadas dentro de 30 dias do recebimento de sua solicitação de acesso. Caso não possamos satisfazer sua solicitação, lhe forneceremos uma explicação por escrito das razões pelas quais precisamos recusar sua solicitação de acesso.

7. Notificação de alterações significativas a esta política

Caso efetuemos uma alteração significativa a esta política ou a nossas práticas de privacidade, publicaremos uma notificação neste website por 30 dias corridos antecedendo a implementação de tal alteração e descrevendo como você poderá exercer qualquer escolha. Após a implementação de tal alteração, registraremos na introdução desta política a data da última revisão. .

8. Como entrar em contato conosco

Perguntas relacionadas a esta política, reclamações sobre nossas práticas e solicitações de acesso deverão ser encaminhadas por e-mail para o endereço (*inserir o endereço de e-mail*) ou por correspondência para (*inserir endereço de correspondência*).

Investigaremos todas as reclamações e procuraremos solucionar aquelas que considerarmos justificadas. Se necessário, alteraremos nossas políticas e procedimentos para garantir que outras pessoas não tenham o mesmo problema.

Colaboração para tradução e adaptação deste material: membros do Conselho de Autorregulamentação da ABEP:

Aurora Yasuda
Laure Castelnau
Maria Luiza de Marco Leal
Mario Mattos
Graziela Thompson
Rubens Hannun
Daniela Chammas Daud
Ana Carolina Franceschi Simões (Coordenação de Comitês ABEP)

Revisão: Tais Bahov



A ESOMAR é a organização mundial para o estímulo, progresso e promoção da pesquisa de mercado ao redor do mundo.

www.ESOMAR.org