GUIA DE PROTEÇÃO DE DADOS – LGPD para Profissionais de Pesquisa de Mercado, Opinião e Mídia

ESOMAR é a porta voz mundial da comunidade de dados, pesquisa e análises, representando mais de 4900 profissionais individuais e 500 empresas que prestam e fazem análises de dados ou pesquisa em mais de 130 países, todos adotando o Código Internacional ICC/ESOMAR

Tradução para o português Duilio Novaes – ABEP
Revisão da tradução por Ana Cássia E. Mercante – IPSOS
Larissa Galvão - Kantar

Revisado em 6 de junho de 2017©

ÍNDICE

1. INTRODUÇÃO

O pesquisador que trabalha num contexto mundial enfrenta, cada vez com mais frequência, um mosaico de leis nacionais desenhadas para assegurar o respeito à privacidade dos indivíduos e a proteção de dados de caráter pessoal. O pesquisador tem a responsabilidade de revisar e cumprir não só os requisitos legais do país em que trabalha, mas também os requisitos nacionais de proteção de dados em todos os países onde realiza uma pesquisa ou tratamento dos dados.

Ao mesmo tempo, a expansão incessante de novas tecnologias em todos os aspectos das nossas vidas não só aumentou o volume dos dados pessoais potencialmente disponíveis para o pesquisador, mas também introduziu novos tipos de informações pessoais que devem ser protegidas.

Algo que não mudou é a necessidade do pesquisador de proteger a reputação da pesquisa de mercado, social e de opinião por meio de práticas que assegurem a transparência com os entrevistados e clientes, que mantenham a confiança na informação que fornecem e que mostrem consideração aos participantes de uma pesquisa.

2. ABRANGÊNCIA

O objetivo deste documento é de proporcionar ao pesquisador, especialmente o que trabalha em pequenas empresas e que podem não dispor de recursos suficientes ou experiência nos requisitos relativos a proteção de dados, uma orientação geral sobre suas responsabilidades dentro de um marco global de proteção de dados, para assegurar que os participantes de uma pesquisa mantenham o controle sobre suas informações pessoais. O marco específico utilizado aqui foi desenvolvido pela Organização para a Cooperação e Desenvolvimento Econômico (*Organisation for Economic Cooperation and Development* - OCDE). Este marco inclui um conjunto de oito princípios para uso e elaboração de programas que assegurem a privacidade e a proteção de dados de caráter pessoal:

- Limites na coleta
- Qualidade de dados
- Especificação da finalidade
- Limites no uso
- Medidas de segurança
- Transparência
- Participação individual
- Responsabilidade

Estes princípios gerais estão refletidos na maior parte da legislação mundial de privacidade e proteção de dados existente e em elaboração.

No entanto o pesquisador deve considerar que os princípios da OCDE são mais alinhados aos requisitos da proteção dos dados da União Europeia, razão pela qual pesquisadores que trabalham em outras regiões são encorajados a consultar outros marcos aplicáveis. Isto inclui Asia-Pacific Co-operation (APEC) Privacy Framework, EU-US Privacy Shield Framework, Suiza-US Privacy Shield Framework e Generally Accepted Privacy Principles (GAPP) desenvolvidos pelo American Institute CPAs (AICPA) e Canadian Institute of Chartered Accountants (CICA). Ainda que estes marcos, em

geral, não tenham força de lei, eles expressam princípios básicos que o pesquisador deve adotar quando trabalhar nestas respectivas regiões.

Ainda, os pesquisadores devem rever e cumprir com os requisitos da autorregulamentação local de proteção de dados e de pesquisa de mercado de cada país onde planeja fazer trabalho de campo ou processamento de dados, uma vez que pode haver diferenças na aplicação dos princípios básicos dentre os países. A orientação contida neste documento consiste em um padrão mínimo e pode necessitar ser complementado com medidas adicionais no contexto de um projeto específico de pesquisa. Os pesquisadores podem considerar necessário contar com assessoria jurídica local, onde a pesquisa será conduzida com a finalidade de garantir sua conformidade. Pode ser útil consultar The Data Protection Laws of the World (As Leis de Proteção de Dados no Mundo), um recurso online, gerenciado por DLA Piper, que é atualizado anualmente.

Por último, o pesquisador que faz pesquisas em áreas especializadas (por exemplo, a pesquisa farmacêutica) pode consultar guias específicos, como o EphMRA Adverse Event Reporting Guidelines 2014 (Guia sobre Comunicação de Eventos Adversos), para mais orientações.

3. Uso do “DEVE” e “DEVERIA”

Neste documento, a palavra “deve” é utilizada para identificar requisitos obrigatórios. Usamos a palavra “deve” para descrever um princípio ou uma prática a qual o pesquisador está obrigado a adotar. A palavra “deveria” é utilizada para descrever uma implementação. Este uso destina-se a reconhecer que os pesquisadores podem optar por usar um princípio ou uma prática de maneiras diferentes, dependendo do desenho da sua pesquisa.

4. DEFINIÇÕES

Atividade não relacionada à pesquisa significa adotar ação direta em relação a um indivíduo, cujos dados pessoais foram coletados ou analisados com a intenção de mudar suas atitudes, opiniões ou ações.

Análise de dados significa o processo de examinar um conjunto de dados para descobrir padrões ocultos, correlações desconhecidas, tendências, preferências e outras informações úteis para fins de pesquisa.

Aviso de privacidade (às vezes mencionado como "política de privacidade") significa um sumário publicado das práticas de privacidade de uma empresa que descreve a maneira como a empresa coleta, usa, divulga e administra os dados pessoais dos indivíduos.

Cliente de pesquisa ou usuário de dados significa qualquer pessoa ou empresa que solicita, comercializa, patrocina ou compra, na totalidade ou em parte, um projeto de pesquisa.

Consentimento significa qualquer manifestação de vontade, livre e informada, de uma pessoa sobre sua concordância com a coleta e tratamento dos seus dados pessoais.

Dano significa dano tangível e material (como um dano físico ou prejuízo financeiro), dano intangível ou moral (como dano à reputação ou ao negócio, ou violação excessiva da vida privada, incluindo mensagens individuais, não solicitadas e de marketing).

Dados pessoais (às vezes chamados de "informação de identificação pessoal" ou "IIP") significa qualquer informação relacionada a uma pessoa (referida como titular dos dados), que pode ser usada para identificar um indivíduo, como por exemplo referência a identificadores diretos (nome, localização geográfica específica, número de telefone, imagem ou gravação de áudio ou vídeo), ou indiretamente por referência a características físicas, fisiológicas, mentais, financeiras, culturais ou sociais dos indivíduos.

Dados primários significa dados coletados por um pesquisador sobre um indivíduo com a finalidade de pesquisa.

Dados secundários significa dados coletados para outra finalidade e subsequentemente utilizados na pesquisa.

Dados sensíveis significa tipos específicos de informação pessoal que a legislação local exige como os mais elevados padrões de proteção contra acesso não autorizado para assegurar a privacidade ou segurança de um indivíduo ou organização e que pode requerer consentimento adicional expresso e inequívoco do titular para que possam ser tratados. A determinação de quais dados são sensíveis varia entre as jurisdições e podem incluir a origem racial ou etnia, registros médicos de saúde, orientação sexual ou hábitos sexuais, antecedentes criminais, opiniões políticas, localização, informação financeira, crenças religiosas ou filosóficas, afiliações sindicais e comportamentos ilegais, tais como o consumo de drogas e álcool.

Operador de Dados significa a pessoa que recebe, registra, mantém ou realiza tratamento (incluído a análise) de dados pessoais em nome e sob a orientação do controlador dos dados. Como se mencionou anteriormente, uma empresa de pesquisa pode ser responsável tanto por tratar como por controlar dados.

Indivíduos vulneráveis significa indivíduos que podem ter limitações em sua capacidade de tomar decisões conscientes e voluntárias, incluindo aqueles com limitações cognitivas ou incapacidade de comunicação.

Interessado significa qualquer indivíduo cujos dados pessoais são usados em pesquisa. Também denominado como “titular dos dados”.

Pesquisa inclui toda pesquisa de mercado, social e de opinião, e análises dos dados; significa o processamento e interpretação sistemática de informações sobre pessoas ou empresas. Utilização de técnicas estatísticas e analíticas das ciências sociais e procedimentos aplicados para gerar perspectivas e apoiar a tomada de decisões dos fabricantes de bens e serviços, governo, ONGs e o público em geral.

Pesquisa business-to-business (B2B) significa a coleta de dados sobre pessoas jurídicas, tais como empresas, escolas, organizações sem fins lucrativos e similares.

Pesquisa business-to-consumer (B2C) significa a coleta de dados de indivíduos.

Pesquisador significa qualquer indivíduo ou organização que conduz um projeto de pesquisa de mercado (ou atua como consultor/freelancer), incluindo os que trabalham na empresa do cliente, assim como todos os subcontratados utilizados.

Legislação que protege a privacidade significa leis ou regulamentos nacionais cujos cumprimentos têm como objetivo proteger os dados pessoais de forma consistente com os princípios estabelecidos neste documento.

Participante da pesquisa (ou **titular dos dados**) significa qualquer pessoa cujos dados pessoais são coletados num projeto de pesquisa, seja por uma entrevista ou por métodos passivos.

Coleta de dados passiva significa dados coletados sem utilizar o sistema tradicional de perguntar e responder às perguntas.

Controlador de Dados significa a pessoa ou a empresa responsável por determinar como os dados pessoais serão tratados. Por exemplo, um cliente da pesquisa poderá ser o controlador dos dados de seus clientes ou consumidores; um órgão governamental de previdência social poderá ser o controlador dos dados coletados de seus beneficiários; um fornecedor de painel de pesquisa será o controlador dos dados coletados dos membros do seu painel online; uma empresa de pesquisa será controladora dos dados coletados dos participantes de uma pesquisa ônibus.

Transferência quando relacionado a dados, se refere a qualquer divulgação, comunicação, cópia ou movimentação de dados de uma parte para outra, independentemente do meio, incluindo, mas não se limitando a transferências por meio de uma rede, transferências físicas, transferências de um meio ou dispositivo a outro, ou por acesso remoto dos dados.

Transferência internacional de dados pessoais significa a movimentação dos dados pessoais para fora do território nacional por qualquer meio, incluindo o acesso a dados de fora do país onde foram coletados e o uso de tecnologia de armazenamento em nuvem de dados.

Tratamento dos dados pessoais inclui, mas não se limita a coleta, registro, organização, armazenamento, adaptação ou alteração, recuperação, consulta, utilização, divulgação por transmissão, distribuição ou qualquer forma de disponibilização, alinhamento ou combinação, bloqueio, supressão ou destruição que seja, por meio automatizado ou por qualquer outro meio.

5. GUIA LIST SOBRE A POLÍTICA E OS PROCEDIMENTOS DE PROTEÇÃO DE DADOS

Os usuários deste *guia* podem notar que os títulos e a sequência dos temas não são os mesmos que foram utilizados pela OCDE. A intenção aqui é mostrar os princípios em uma linguagem e ordem mais familiar para os pesquisadores. Os usuários também poderão ver que os temas estão inter-relacionados e as vezes se sobrepõem. **No entanto é essencial que este *guia* seja visto como um todo, e que os temas individuais sejam vistos como complementares e não como excludentes, prestando principal atenção nas diferenças que dependerão da atuação da empresa quer como controladora de dados, quer como operadora de dados. Qualquer pergunta para a qual a resposta não seja um "sim" indica uma potencial brecha no programa de proteção de privacidade e, portanto, um potencial risco de violação a uma ou a mais leis de proteção dos dados.**

5.1 Impacto mínimo

1. *Ao desenhar um projeto de pesquisa, você limita a coleta de dados pessoais apenas àqueles itens necessários para os propósitos da pesquisa e assegura que eles não serão utilizados de maneira incompatível com tais propósitos?*

O pesquisador somente deve coletar, adquirir e/ou manter dados pessoais necessários sob a perspectiva de controle de qualidade, amostragem e/ou análise. No caso de pesquisa B2B, o procedimento inclui os dados pessoais relativos ao cargo ou ao nível do respondente dentro da empresa, desde que sejam necessários para o objetivo da pesquisa.

Este mesmo princípio se aplica aos métodos passivos de coleta de dados, assim como quando se trabalha com fontes de dados secundários. Então, é responsabilidade do pesquisador assegurar que os dados pessoais a serem utilizados na pesquisa sejam apenas aqueles necessários aos propósitos da pesquisa. Caso venha a receber outros dados pessoais, estes devem ser filtrados e eliminados.

2. *Você implementa processos que assegurem que os participantes da pesquisa não sejam prejudicados ou afetados negativamente como resultado direto de seus dados pessoais estarem sendo utilizados em uma pesquisa de mercado?*

O pesquisador deve assegurar que os dados pessoais não possam ser rastreados e que não possam identificar a uma pessoa mediante análises cruzadas (divulgação dedutiva), amostras pequenas ou por qualquer outra forma através dos resultados da pesquisa. Exemplos disso seriam a agregação de informações auxiliares, como uso de dados de zona geográfica ou a capacidade de identificar um empregado específico em uma entrevista de satisfação de cliente.

3. *Se você planeja utilizar subcontratados ou outros fornecedores para prestar os serviços em seu nome, você fornece o mínimo de informação pessoal necessária para que possam realizar os serviços que serão prestados? Você formaliza contratos que garantam um nível adequado de proteção para estes dados?*

Quando contratar um subcontratado, forneça apenas a quantidade mínima de dados pessoais que sejam necessários para realização do projeto contratado, sempre deixando claro, por meio de contratos e de instruções, quais são as responsabilidades do subcontratado enquanto estiver de posse dessas informações/dados. Todos os subcontratados devem utilizar as mesmas normas e regulamentos que a empresa de pesquisa utiliza. Ainda, a transferência de dados pessoais a um subcontratado ou outro fornecedor só deve ser realizada com o prévio consentimento ou por solicitação do cliente da empresa de pesquisa.

O parágrafo anterior supõe que os dados coletados na pesquisa serão mantidos de forma confidencial e só serão analisados e divulgados em nível agregado. Quando os participantes da pesquisa derem seu consentimento para a vinculação das suas respostas aos seus dados pessoais, eles deverão ser informados de como seus dados serão compartilhados e utilizados.

5.2 Notificação e Consentimento

4. *Quando se coletam dados primários, você obtém o consentimento de cada um dos participantes da pesquisa cujos dados pessoais serão coletados?*

Conforme os Princípios de Privacidade da OCDE, qualquer dado pessoal deve ser obtido por meios legítimos e justos e, neste caso, com o conhecimento ou consentimento do participante na pesquisa. Em geral, a legislação nacional estabelece uma série de fundamentos legítimos e justos, mas, na maioria dos casos, o pesquisador estará obrigado a obter o consentimento.

O consentimento deve ser:

- livre (voluntário e em condições de ser retirado a qualquer momento);
- específico (em relação a uma ou mais finalidades identificadas); e
- informado (com pleno conhecimento relativo às possíveis consequências decorrentes do consentimento).

O consentimento também deve ser claramente indicado por uma declaração ou ação por parte do participante da pesquisa (titular dos dados) que tenha sido informado do seguinte: (a) o uso que se fará de seus dados pessoais; (b) os dados específicos que serão coletados; (c) o nome, endereço e a informação de contato da empresa ou organização que coletará os dados e, se não for a mesma, do controlador dos dados; e (d) se os dados serão divulgados a terceiros.

O pesquisador deve considerar cuidadosamente o mecanismo utilizado para obtenção do consentimento, normalmente como *opt-out*, *opt-in*, implícito, informado ou explicito. O método específico escolhido deve estar documentado.

Em geral, quanto mais sensível, invasiva ou não evidente é a coleta de dados, mais elevado deve ser o padrão de consentimento a ser obtido. Em algumas jurisdições existem tipo de “dados pessoais sensíveis” que requerem o consentimento expresso das pessoas afetadas antes que os dados possam ser coletados.

Pode haver casos em que o pesquisador colete ou receba dados pessoais de forma não intencional ou de pessoas que não são participantes da pesquisa. Por exemplo: informação oferecida voluntariamente pelos participantes; listas fornecidas pelo cliente que contém mais informação que seriam necessárias para a realização da pesquisa; e transeuntes ou espectadores capturados por fotografias ou vídeos. O pesquisador deve tratar estas informações da mesma forma com que trata os outros dados pessoais. Tais dados devem ser anonimizados ou descartados de imediato, especialmente se não houver como informar às pessoas cujos dados foram coletados, sobre sua finalidade, armazenamento ou utilização. Em algumas jurisdições é obrigatório apagar estas informações ou tratar da mesma forma que as outras informações obtidas intencionalmente.

5. *Você é transparente em relação a finalidade ou às finalidades para as quais os dados foram coletados e armazenados?*

Há muito o setor de pesquisa sustenta uma diferença entre a pesquisa de mercado e a compilação de dados para outros fins, tais como publicidade, promoção de vendas, elaboração de bases de

dados, marketing direto e venda direta. Esta diferenciação é um fator crítico para a distinção da finalidade e para a promoção de uma imagem positiva da pesquisa aos olhos dos legisladores e do público em geral. Nos últimos anos, com o aparecimento de novas tecnologias, aumentaram as oportunidades para coleta de informações pessoais através de técnicas como monitoramento online e aplicativos baixados em celulares. Em qualquer caso, é essencial que, antes de coletar qualquer dado, os possíveis titulares dos dados sejam informados sobre a finalidade para as quais seus dados serão utilizados sobre qualquer consequência potencial que pode resultar desta coleta, incluindo a finalidade de um contato para o fim de controle de qualidade.

Quando o pesquisador coleta dados pessoais de um participante de pesquisa para ser utilizada com a finalidade de pesquisa de mercado, a transparência para com o titular dos dados é um fator crítico a ser comunicado a ele. Ao participante da pesquisa deve se dar informação suficiente sobre o uso previsto dos dados pessoais coletados e toda informação sobre compartilhamento desses dados com terceiros. Por exemplo: se o uso previsto dos dados é vincular as respostas de uma entrevista ao perfil do cliente, o participante da pesquisa deve ser informado disso no momento da coleta dos seus dados pessoais.

Os avisos de privacidade devem ser revisados frequentemente para garantir que o tipo dos dados coletados e seus usos previstos não foram alterados, e o pesquisador deve se assegurar que as práticas da empresa e as tecnologias utilizadas na empresa de pesquisa são consistentes com os compromissos firmados com os participantes das pesquisas, e que cumprem os requisitos acordados e vigentes a cada momento/projeto. Cada uso proposto de dados pessoais deve ser analisado para garantir o cumprimento da legislação local sobre privacidade, do Código Internacional ICC/ESOMAR e dos Guias de ESOMAR/GRBN e toda a coerência dos compromissos de privacidade assumidos com as partes interessadas.

6. *Você é transparente sobre os dados específicos que serão coletados?*

Dada a ampla definição de dados pessoais em algumas jurisdições, devem ser considerados todos os possíveis elementos de dados pessoais que podem ser coletados no momento da redação da informação aos titulares de dados. Dados pessoais podem incluir nome, endereço, e-mail, número de telefone, número de celular, data de nascimento, identificador de celular, endereço de IP, fotografias, gravações de áudio e vídeo, RG, CPF, CNH, Carteira Profissional etc., crachá da empresa, nome do usuário nas redes sociais, dados armazenados em cookies ou pixel/marcação para seguir. Lembre-se também que um só elemento de dado, por si só, pode não ser considerado como dado pessoal identificável conforme a legislação local, mas quando combinado com outros dados (por exemplo, cep, sexo, local de trabalho ou escola, cargo e salário), pode permitir que uma pessoa possa ser identificada individualmente.

Adicionalmente, considere todos os possíveis destinatários de dados pessoais. Pesquisadores, empresas de pesquisa, fornecedores de serviços e/ou os clientes finais podem ter a capacidade de coletar e/ou utilizar os dados pessoais em um projeto de pesquisa.

7. *Você deixa claro como serão coletados os dados, incluindo qualquer tipo de coleta passiva em que o titular dos dados pode não ter ciência?*

Historicamente, a pesquisa se apoiou na entrevista como método principal para a coleta de dados pessoais. Como mencionado no item 5 acima, novas tecnologias possibilitam a coleta de uma gama mais ampla de dados pessoais sem o conhecimento das pessoas cujos dados são coletados. Todos os titulares de dados devem ser informados sobre quais dados seus específicos estão sendo coletados e o(s) método(s) de coleta que está(ão) sendo utilizados, seja por um meio ativo como em uma entrevista, ou por um meio passivo tal como um aplicativo de celular ou um acompanhamento de comportamento *online* através de cookies.

O pesquisador deve considerar quais elementos dos dados coletados e/ou o método de coleta de dados podem não ser do conhecimento do participante de pesquisa e fornecer informação clara em relação aos métodos de coleta. Considere o uso de "avisos abreviados" capeando avisos de privacidade mais detalhados para descrever a coleta ou o uso de dados que poderia ser inesperado ou invasivo. Aplicativos de celulares, em particular aqueles que incluem geolocalização, "escuta passiva" e/ou medição dos dispositivos do sistema operacional do celular requerem uma descrição detalhada e o consentimento explícito do titular dos dados autorizando essas atividades.

8. *Quando utilizar dados pessoais coletados para outra finalidade que não a pesquisa (por exemplo, dados de clientes, dados de redes sociais etc.), você se assegura de que o uso é legítimo e de que os direitos dos titulares de dados estão protegidos?*

Pesquisadores e não pesquisadores buscam cada vez mais obter e usar dados secundários para aumentar ou substituir a coleta primária de dados. Antes de acessar e tratar tais dados, o pesquisador deve se assegurar de que o uso planejado é compatível com a finalidade para a qual tais dados foram coletados. Deve-se verificar se a coleta original foi legal e com o consentimento dos titulares de dados, expresso ou implícito. Também deve-se determinar o interesse legítimo, assegurando que a finalidade é unicamente para pesquisa.

Ainda, o pesquisador deve planejar sua pesquisa de forma que o tratamento subsequente dos dados não resulte em riscos de danos aos participantes da pesquisa. O pesquisador deve tomar cuidados para mitigar o risco de danos, assegurando que a identidade do participante da pesquisa não seja descoberta ou divulgada sem seu prévio consentimento, adotando medidas para reduzir a granularidade dos dados de forma a reduzir a possibilidade de identificação do indivíduo, e assegurando que uma atividade não relacionada à pesquisa seja direcionada ao participante em decorrência direta de sua participação na pesquisa.

5.3 Integridade/Segurança

9. *Você adota procedimentos para garantir que todos os dados pessoais coletados sejam exatos, completos e atualizados?*

Controles de qualidade devem ser realizados em cada etapa do processo de pesquisa. No desenho dos questionários ou aplicações da pesquisa, devem ser realizados pré-testes antes do início dos trabalhos de campo para minimizar o risco de erros na coleta de dados. Durante os trabalhos de campo, o monitoramento e validação das entrevistas devem ser feitos conforme as normas de qualidade aplicáveis no tipo da pesquisa/metodologia. Durante o processamento de dados e a apresentação dos resultados, devem ser feitos controles de qualidade adicionais para assegurar que os dados estão corretos e que a análise, conclusões e recomendações são consistentes aos dados.

O pesquisador que gerencia painéis deve garantir que os panelistas possam rever e atualizar seus dados de perfil a qualquer momento e devem lembrá-los, periodicamente, que os façam. As amostras extraídas de um painel devem conter informações sociodemográficas atualizadas. Para isso, uma boa fonte para consultar boas práticas é o *ISO 26362:2009 Acess panels in Market*, *opinion and social reserach.*

Ao utilizar dados secundários, o pesquisador deve rever o controle de qualidade aplicado no momento da coleta para se assegurar de que os dados sejam precisos.

10. *Você assegura que os dados pessoais não serão mantidos por tempo superior ao que o necessário para a finalidade para a qual a informação foi coletada, obtida ou tratada? Você tem procedimentos para armazenar separadamente ou eliminar os dados de identificação dos bancos de dados quando eles não forem mais necessários?*

O pesquisador deve estabelecer os períodos mais curtos possíveis para reter os dados, mas sempre observando a na legislação aplicável *(no caso do Brasil, a Lei nº 12.965/13, conhecida como Marco Civil da Internet, estabelece o prazo de 1 ano de retenção dos dados)*, a fonte dos dados pessoais coletados e a condição de sua atuação como controlador ou operador dos dados. Neste último caso, os clientes podem impor por contrato períodos de retenção.

Em relação à fonte dos dados pessoais, a informação de projetos longos ou a informação de perfil dos panelistas normalmente serão usadas e retidas durante todo o tempo em que permanecerem como membros ativos. Por outro lado, o período de retenção deve ser mais curto para dados pessoais de participantes de pesquisa que não sejam panelistas e que participem de uma pesquisa *ad-hoc*. Obviamente, é importante não eliminar dados pessoais de imediato, já que controles de qualidade devem ser realizados durante o tratamento dos dados para assegurar a exatidão e satisfazer as exigências dos princípios de integridade da privacidade dos dados.

Quando se utilizam dados pessoais, é uma boa prática para o pesquisador usar identificadores através de pseudônimos/códigos. Deve-se manter de forma segura e com acesso limitado ao menor número de pessoas possível (por exemplo, o pessoal de gerenciamento do painel ou de elaboração de amostras), um arquivo mestre onde se associa os nomes, endereços ou números de telefone dos participantes de pesquisas com seus respectivos números de identificação gerados internamente. Assim, os pesquisadores, o pessoal de processamento de dados ou de codificação que necessitem analisar os dados individualmente, poderão fazê-lo sem ver os nomes, endereços ou números de telefone dos titulares de dados.

Quando as respostas do estudo forem processadas e apresentadas com dados estatísticos agregados, os dados pessoais dos participantes de pesquisa, junto com suas correspondentes identificações através de pseudônimos/códigos, devem ser eliminados, de modo que a empresa de pesquisa não mantenha os dados pessoais.

11. *Há procedimentos estabelecidos para responder as solicitações dos titulares de dados relativas aos dados pessoais que você mantém deles? Os procedimentos para lidar com os pedidos de acesso dos titulares de dados incluem a autenticação da identidade do solicitante, respostas às solicitações em um período de tempo razoável, permissão para correção de dados errados ou eliminação completa dos dados?*

Procedimentos formais devem ser desenvolvidos, comunicados e seguidos para responder a titulares de dados que desejem acessar os dados que a empresa mantém sobre eles. A autenticação (comprovação) do titular do dado que solicita o acesso é importante para evitar divulgar dados a outras pessoas indevidamente.

Uma vez que a identidade do participante da pesquisa que solicitou o acesso tenha sido comprovada – a pessoa é quem diz ser e tem o direito legítimo de acessar os dados pessoais em questão – o pesquisador deverá esforçar-se para atender à solicitação de acesso o mais rápido possível, por exemplo, dentro de 10 a 30 dias, dependendo da legislação aplicável. Se a empresa de pesquisa precisar de um tempo adicional para atender à solicitação, e seja possível estender o prazo estabelecido na lei, o solicitante deve ser informado e as razões específicas para se estender o prazo expostas. O prazo adicional pode ser necessário, por exemplo, para realização de consultas ou para reunir as informações de várias bases de dados ou fontes.

Ainda que a legislação de proteção de dados inclua exceções que obriguem as empresas a negar o acesso às suas informações ao titular de dados em algumas situações, provavelmente essas exceções não são aplicáveis a dados pessoais processados para fins de pesquisa. Por exemplo, a legislação aplicável pode permitir à empresa negar solicitações de acesso se a informação estiver sujeita a confidencialidade entre advogado e cliente. Outro exemplo poderia ser a empresa ter comunicado a informação a um órgão governamental para cumprimento da lei ou de segurança nacional, este órgão pode instruir a empresa a negar o acesso ou não revelar que a informação lhe foi enviada.

12. *Há protocolos de segurança estabelecidos para cada conjunto de arquivos de dados de forma que os proteja contra riscos tais como a perda, acesso não autorizado, destruição, uso, modificação ou divulgação.*

O cumprimento destas responsabilidades começa com o desenvolvimento e implementação de uma política de segurança para proteger informações pessoais outros tipos de informações confidenciais. ISO 27001 é uma norma reconhecida de segurança da informação numa política de segurança ampla em que poderá ser baseada.

O uso de medidas de segurança apropriadas para fornecer a proteção necessária inclui:

- medidas físicas (arquivos trancados a chave, acesso restrito nos recintos/escritórios, sistema de alarme, câmeras de segurança);
- ferramentas digitais (senhas, encriptação, firewalls)
- controles na empresa (verificação de antecedentes, normas relativas a tirar arquivos para fora das instalações, limitar acesso sobre a base de dados a “necessidade de conhecer”, formação de pessoal, acordos com clientes e subcontratados).

A política de segurança deve incluir também um procedimento para lidar com uma possível violação de segurança dos dados na qual dados pessoais são divulgados. Se forem dados secundários coletados por terceiros, por exemplo, uma base de dados de um cliente, este terceiro deve ser informado imediatamente. Os titulares de dados violados também devem ser informados se esta violação os exponha a algum risco (por exemplo, o roubo de identidade) e quais as medidas adotadas para proteger contra o risco.

13. Há uma declaração clara sobre o prazo de retenção dos dados pessoais.

O prazo para conservação dos dados pessoais pode variar de um projeto de pesquisa para outro dependendo de uma série de circunstâncias indicadas anteriormente na resposta à pergunta 9.

Ainda que as normas gerais sobre os prazos de retenção possam estar incluídas nos avisos de privacidade, pode não ser prático informar precisamente diferentes prazos de retenção para os diferentes tipos de pesquisa. Portanto, o pesquisador também deve considerar comunicar a informação sobre retenção de dado no instrumento de captação do estudo, na introdução do questionário ou em formulários para obtenção do consentimento específico do estudo. Sempre se deve estar preparado para informar os prazos de retenção dos dados de um projeto determinado quando solicitado.

5.4 Transferência de dados

14. Você tem normas e procedimentos definidos que determinam o uso e divulgação dos dados pessoais?

Estas regras e procedimentos estão claramente descritos na legislação local sobre privacidade e proteção dos dados que existe em seu país. Uma explicação do que isso significa deve estar claramente documentada junto aos processos e documentos escritos para assegurar que a equipe aplique os protocolos relativos a como gerenciar dados pessoais e para que a equipe esteja familiarizada com estas normas e procedimentos. Por exemplo, isto inclui o princípio de que o consentimento do participante da pesquisa deve ser obtido antes que seus dados possam ser divulgados, inclusive aos clientes ou aos pesquisadores da empresa do cliente, independentemente se os dados foram coletados pelo pesquisador ou por um terceiro.

15. As condições sob as quais os dados pessoais podem ser divulgados está clara e sem ambiguidades?

Os titulares de dados devem saber o que será feito com seus dados pessoais e isto deve ser explicado verbalmente ou mediante algum tipo de formulário ou documento escrito no qual será obtido o consentimento do titular do dado – que quer dizer, via seu consentimento fica registrado como evidência que concordou.

16. Sua equipe está ciente e treinada sobre como aplicar os procedimentos?

Sua política de privacidade descreve as práticas de coleta e gestão de dados em sua empresa. É igualmente importante desenvolver procedimentos operacionais internos padronizados (SOP's) para assegurar que se cumpram os compromissos de privacidade junto aos titulares de dados.

O treinamento de uma equipe sobre privacidade deve incluir uma visão geral da legislação aplicável, dos códigos de conduta setoriais, das políticas de privacidade de sua empresa para o consumidor e seus procedimentos operacionais internos padronizados. O treinamento deve ser dado ao menos uma vez ao ano e registros de comparecimento devem ser mantidos.

Toda a equipe da linha de frente que interage com os titulares de dados deve ser capaz de explicar com detalhes as políticas e procedimentos da sua empresa. Devem saber a quem se dirigir internamente para obter ajuda em caso de dúvidas que não sejam capazes de responder.

Deve haver clara supervisão e responsabilidade delineada, incluindo uma forma de comprovar que os procedimentos estão sendo cumpridos.

5.5 Transferência internacional de dados pessoais

17. A transferência de dados pessoais de uma jurisdição a outra, deve ser feita de tal maneira que se cumpram com os requisitos de proteção de dados tanto na jurisdição de origem como na de destino.

Isso é frequentemente chamado de "transferência internacional de dados pessoais". Ocorre quando os dados são coletados fora das fronteiras nacionais e/ou quando o tratamento dos dados é realizado ou subcontratado para realização em outro país (por exemplo, quando um cliente pede a um pesquisador em outro país para conduzir um estudo com dados fornecidos por um consumidor de seu país). Cada país tem suas próprias normas sobre como devem ser tratados e protegidos os dados pessoais, normas que o pesquisador deve cumprir. Enquanto isso pode parecer complexo, ajudará se as questões de *compliance* enfrentadas pelo pesquisador forem divididas em três grandes tópicos:

- Assegurar-se de que a transferência internacional dos dados será realizada em conformidade com a legislação nacional e internacional, regulamentos e normas aplicáveis. A base legal mais comum para assegurar a proteção adequada em uma transferência internacional é mediante o consentimento dado pelo titular dos dados ou mediante o uso de cláusulas contratuais apropriadas e, quando exigido pela legislação nacional aplicável, mediante a obtenção da autorização prévia da Autoridade Nacional de Proteção dos Dados ou de outra autoridade reguladora de privacidade aplicável para o uso desses contratos. Como medida adicional de segurança e para reduzir ainda mais os riscos quando o tratamento de dados for realizada em outro país, dados que permitam a identificação do indivíduo devem ser removidos sempre que possível, a fim de que somente números de identificação sinonimizados/codificados sejam utilizados para vincular o indivíduo à sua identidade.
- O limite a ser observado pelo pesquisador que for realizar a transferência internacional atuando como operador de dados, como por exemplo quando se faz um estudo utilizando amostra fornecida pelo cliente. Mesmo quando o pesquisador tomou a precaução para garantir que todas as transferências cumprem as normas que regulam a transferência internacional, também deve ser levado em conta sua atuação como operador dos dados (quer dizer, quando atua em nome de um controlador, por exemplo o cliente da pesquisa), já que o controlador pode não ter a permissão para realizar a transferência internacional de dados pessoais pelos quais é responsável, o que pode afetar a forma de condução do projeto. Deve-se fazer um contrato escrito entre ambas as partes sobre a sugestão acima.
- A transferência internacional de dados envolvendo titulares de dados situados em outros países, (por exemplo, em entrevistas online dirigidas a titulares de dados que residam em um outro país que não o que o pesquisador está conduzindo o estudo). A legislação aplicável sobre privacidade normalmente será a do país em que pesquisador está fazendo a pesquisa. No entanto o pesquisador deve se assegurar de que o estudo ou o painel é conduzido nos termos de qualquer outra legislação nacional aplicável, no país onde os dados são coletados.

As práticas recomendadas incluem assegurar-se de que: (1) em todo instrumento de captação deve-se informar claramente os dados do pesquisador (razão social da empresa, endereço, etc.) incluindo o país; (2) a política de privacidade divulgada *online* inclua uma declaração simples, mas clara e inequívoca, sobre a possível transferência internacional que poderá resultar da participação do estudo por meio de painel; (3) haja referência à transferência internacional de dados na pergunta para obtenção do consentimento para o integrante do painel.

5.6 Terceirização e subcontratação

18. *Há requisitos claros, incluindo controles adequados, para casos de terceirização ou subcontratação de operadores de dados?*

Deve-se informar claramente os requisitos a todos os operadores de dados terceirizados ou subcontratados, relativos ao cumprimento das normas de proteção dos dados aplicáveis aos dados pessoais quando os dados são transferidos por qualquer tipo de meio. Deve haver uma proteção adicional na transmissão dos dados, seja em nível individual ou agregado, com o uso de processos digitais específicos de TI, tais como encriptação de dados transferidos ou uso de plataformas de transferências FTP (File Transfer Protocol) seguras. Se os subcontratados ou terceiros fizerem cópias de segurança de qualquer dado, deve haver regras e procedimento específicos para proteger estes dados durante o armazenamento e para sua eliminação quando já não forem mais necessários.

19. *Você tem um acordo (contrato) vigente com todos os seus subcontratados.*

Deve ser firmado contrato com qualquer subcontratado envolvido. O contrato deve conter os termos comerciais do trabalho a ser feito (incluindo uma descrição das tarefas, prazos, seguros etc.) assim como:

- requisitos de proteção dos dados; e
- requisitos de segurança da informação.

5.7 Política de Privacidade

20. *A informação sobre sua política de privacidade e normas de proteção dos dados pessoais está prontamente disponível e de uma forma que seja facilmente compreensível para os participantes?*

Muitas jurisdições requerem que a informação esteja disponível em um aviso de privacidade que esteja prontamente disponível para os titulares de dados. Ainda que o conteúdo e detalhes exigidos variem de um país para outro, o pesquisador deve sempre se identificar claramente aos titulares de dados e assegurar-se de que será explicado a finalidade da pesquisa, como os dados pessoais serão coletados, a forma que as informações serão gerenciadas (coleta, armazenamento, uso, acesso e divulgação), e como serão obtidas mais informações ou apresentada uma queixa.

O pesquisador deve se assegurar que as políticas são fáceis de entender, relevantes para o leitor, fáceis de localizar, tão concisas quanto possível e adaptadas aos negócios da empresa. Isso inclui ter

a política em tantas línguas quanto sejam necessárias e revisar e atualizar a política quando necessário.

21. A identidade e a responsabilidade do controlador dos dados está clara?

O pesquisador deve se assegurar que suas próprias regras e responsabilidades no gerenciamento dos dados pessoais estejam claras para os titulares de dados. Isto inclui a identificação do controlador de dados e se você utilizará algum operador de dados terceirizado. Os titulares de dados não poderão ter dúvidas de que a empresa é a responsável em última instância pelo gerenciamento de seus dados.

Algumas jurisdições também pedem que uma pessoa específica seja indicada como responsável pelos processos de proteção de dados na empresa.

No caso de entrevistas "blind" nas quais se utilizam amostras fornecidas pelo cliente, os participantes devem ser informados no início da entrevista que o nome do cliente não será revelado até o final da entrevista uma vez que esta informação sendo fornecida antecipadamente, poderá acarretar um viés nas respostas. Uma vez que em muitos casos a legislação nacional de proteção de dados concede o direito aos titulares de dados de saber de quem o pesquisador obteve seus dados pessoais, o pesquisador deve estar preparado para informar o nome do cliente em qualquer momento em que for solicitado pelos participantes.

22. Está claro que o controlador dos dados é o responsável pelos dados pessoais que estão sob sua guarda, independentemente da localização dos dados?

Se o pesquisador tiver a intenção de subcontratar o tratamento, ou transferir os dados pessoais para fora de seu país, ele deverá estar preparado para informar ao controlador dos dados os detalhes dos subcontratados e a localização onde será realizado o tratamento de dados e obter o consentimento prévio por escrito do controlador de dados quando necessário. Quando a empresa de pesquisa é a controladora de dados, deverá incluir referências à utilização pelo operador de dados e, neste caso, uma lista dos países ou regiões na sua política de privacidade. O pesquisador deve estar atento ao fato de que em algumas jurisdições proíbem os pesquisadores de fazer a transferência internacional de dados pessoais a países ou regiões na qual não haja legislação com um nível equivalente de proteção de dados. Obrigadas ao cumprimento das regras que regem a transferência internacional impostas pela legislação nacional local relevante, a transferência da informação pessoal dentro de empresas multinacionais é permitida na maioria das jurisdições, ainda que em alguns países seja necessário informar aos titulares de dados sobre onde podem ser utilizados seus dados.

6. Questões Especiais

6.1 Coleta de dados de crianças, pessoas jovens e outras pessoas vulneráveis:

O pesquisador deve obter o consentimento do pai/mãe ou responsável/tutor legal antes de coletar dados pessoais de quaisquer titulares de dados a quem lhe foi atribuído um tutor legal. Quando se solicita o consentimento, o pesquisador deve fornecer informação suficiente sobre a natureza do projeto de pesquisa de forma que permita ao pai/mãe ou responsável/tutor legal tomar uma decisão sobre a participação do titular de dado. Isto inclui:

- o nome e os dados de contato do pesquisador ou organização que está fazendo a pesquisa;
- a natureza dos dados que serão coletados do titular do dado;
- uma explicação de como serão usados e protegidos esses dados;
- uma explicação das razões porque foi solicitada sua participação e os possíveis benefícios ou impactos;
- uma descrição dos procedimentos para reforçar e checar o consentimento; e
- a solicitação dos dados de contato (endereço ou telefone) do pai/mãe ou responsável/tutor legal para a verificação do consentimento.

O pesquisador também deverá registrar a identidade do responsável/tutor e sua relação com o titular de dado.

Atualmente não existe uma definição comum internacional do que é uma criança ou pessoa jovem. Inclusive dentro de um mesmo país a definição pode variar. Estabelecer uma definição alternativa baseada em características definidas de idade (por exemplo, capacidades cognitivas) para aplicar em uma pesquisa é difícil, senão impossível. Por isso o pesquisador deverá embasar-se em qualquer definição relevante descrita pela legislação local, pelos códigos de conduta e pelas normas culturais. Se não houver estas diretrizes claras, ESOMAR e GRBN *assim como a legislação brasileira* recomendam definir crianças como menor de 12 anos e pessoas jovens, como a pessoa entre 13 e 17 anos. Para maiores detalhes consulte o Guia ESOMAR para entrevistas com crianças e jovens.

6.2 Pesquisa business-to-business

Um número considerável de projetos de pesquisa inclui a coleta de dados de pessoas jurídicas tais como empresas, escolas, organizações sem fins lucrativos e organizações similares. Tais pesquisas frequentemente envolvem a coleta de informações sobre a entidade, por exemplo: faturamento, número de empregados, setor de atuação, localização etc.

Em todos estes casos as empresas participantes têm o direito ao mesmo nível de proteção em relação à revelação de sua identidade/dados que são oferecidas as pessoas/indivíduos em outros tipos de pesquisa.

Vale a pena salientar que em muitos casos a legislação nacional de proteção de dados considera que o cargo e os dados de contato do local de trabalho de uma pessoa são dados pessoais. Algumas leis de proteção de dados vão mais além e consideram suas exigências a serem aplicadas tanto para as pessoas físicas como jurídicas (por exemplo, pessoas individuais e empresas).

6.3 Fotografias, gravações de áudio e vídeo

Várias técnicas novas de pesquisa captam, armazenam e transmitem fotografias e gravações de áudio e vídeo como parte do processo de pesquisa. Dois exemplos destacados são a pesquisa etnográfica e os estudos de cliente misterioso (mystery shopping).

O pesquisador deve se dar conta que as fotografias e as gravações de áudio e vídeo são dados pessoais e deve ser tratados como tais. Se o pesquisador pede aos titulares de dados que forneçam

informações nesse formato, também deverão fornecer orientação sobre como descartar a coleta de dados não solicitados, especialmente em relação aos não participantes.

Por último, em alguns tipos de pesquisa por observação pode ocorrer a fotografia, a filmagem e a gravação em lugares públicos de forma que afetem as pessoas que não foram escolhidas como titulares de dados. Em tais casos, o pesquisador deve obter a permissão para compartilhar este tipo de imagem daquelas pessoas cujo rosto são claramente visíveis e podem ser identificadas. Se não conseguir obter a permissão, então a imagem da pessoa deve ser borrada ou anonimizada de alguma forma. Ainda, deveremos colocar cartazes claros e legíveis para indicar que a região está sob observação, junto com os dados da pessoa ou organização responsável. As câmeras devem estar colocadas de forma que só filmem as regiões definidas.

6.4 Armazenamento em nuvem

A decisão de armazenar os dados pessoais em nuvem deve ser pensada cuidadosamente. O pesquisador deve avaliar os controles de segurança do fornecedor de serviços de armazenamento em nuvem e seus padrões, termos e condições. Muitos fornecedores de serviço de armazenamento em nuvem oferecem indenizações ínfimas no caso de ocorrerem violações de segurança quando os dados pessoais forem comprometidos. Isto significa que a empresa de pesquisa estaria assumindo um risco considerável pelos danos financeiros e perdas referentes as violações graves da privacidade que resultem em danos aos titulares de dados afetados.

Portanto, o pesquisador deve implementar controles e compensações para se proteger contra esses riscos. Por exemplo, deveria encriptar os dados pessoais na transferência (transferidos para nuvem) e para guardá-los (armazenados nos servidores do fornecedor em nuvem). O pesquisador também deverá considerar a contratação de uma apólice de seguro de responsabilidade digital.

O pesquisador deve também levar em conta a localização física onde se armazenam os dados pessoais para determinar se o uso de armazenamento na nuvem seja uma transferência internacional. Consultar a seção 5.5 deste documento para mais informações. Alguns fornecedores de serviços de armazenamento em nuvem oferecem lugares de armazenamento específico em país que podem ser apropriados para alguns casos.

Por último, o pesquisador deverá armazenar os dados pessoais em uma nuvem privada em vez de uma pública. A nuvem privada é a que atribui um centro de dados particular, equipamento digital exclusivo para a empresa do pesquisador. O principal benefício de uma nuvem privada é que o pesquisador sempre saberá onde se encontram os dados pessoais. Ao contrário que em uma nuvem pública pode ocorrer que os dados estejam armazenados em dois ou mais centros de dados e em dois ou mais continentes, com a possibilidade de surgirem problemas de cumprimento, tanto dos requisitos aplicáveis de acordo com a legislação de proteção de dados como dos contratos assinados com os responsáveis do tratamento, que especificam onde se deve armazenar os dados pessoais.

6.5 Dados Anonimizados e Sinonimizados

Uma parte importante da responsabilidade da proteção dos dados de um pesquisador é eliminar a identificação dos dados antes de sua liberação a um cliente ou inclusive ao público em geral. O processo de anonimizar é uma garantia que implica no apagamento ou modificação dos dados de

identificação pessoal resultando em dados que não identifiquem as pessoas. Alguns exemplos incluem esfumaçar as imagens para descaracterizar os rostos ou entregar os resultados como agregação estatística para assegurar que não se possa identificar uma pessoa em particular.

Sinonimizar implica na modificação dos dados pessoais de tal maneira que ainda seja possível distinguir as pessoas em um conjunto de informações mediante um identificador único (por exemplo com um número de identificação ou com algoritmos de modificação), enquanto são mantidos os dados pessoais separados para fins de controle. (ver P9).

Quando se utilizam estas técnicas, o pesquisador deve consultar a legislação nacional e os códigos locais de autorregulamentação para determinar quais elementos devem ser eliminados para satisfazer os requisitos legais nos processos de anonimização/sinonimização dos respectivos dados.

7. Fontes e Referências

DLA Piper, Data Protection Laws of the World
EphMRA Adverse Event Reporting Guidelines 2014
Código Internacional ICC/ESOMAR Para a Prática de Pesquisa Social e de Mercado
Guia ESOMAR para entrevistas com crianças e jovens
ISO 26362:2009 – Access panels in market, opinion, and social research
Esquema de Privacy Shield
OCDE Princípios de Privacidade

8. Equipe do Projeto

Co presidentes:

- Reg Baker, Consultor del Comité de Normas Profesionales de ESOMAR y Marketing Research Institute International
- David Stark, Vice-presidente, Integrity, Compliance and Privacy, GfK

Membros da equipe do projeto:

- Debrah Harding, Director General, Market Research Society
- Stephen Jenke, Consultor
- Kathy Joe, Director de International Standards and Public Affairs, ESOMAR
- Wander Meijer, COO Global, MRops
- Ashlin Quirk, Consejero General en SSI
- Barry Ryan, Gerente, Global Privacy - Program, Policy & Governance, American Express
- Jayne Van Souwe, Director, Wallis Consulting Group