GUIA DE PROTEÇÃO DE DADOS PESSOAIS

PESQUISA

NOVEMBRO, 2020

FICHA TÉCNICA

Guia de Proteção de Dados Pessoais – Pesquisa
Versão 1.0, novembro de 2020

PROJETO DE CONFORMIDADE À LEI DE PROTEÇÃO DE DADOS PESSOAIS

Diretoria de Controles Internos - DCI

Maria Alice da Justa Lemos - Diretora de Controles Internos

Centro de Ensino e Pesquisa em Inovação – CEPI (FGV Direito SP)

Coordenação Técnica

Alexandre Pacheco da Silva

Coordenação Executiva

Victor Nóbrega Luccas

Equipe de Pesquisadores

Fábio Ferraz de Almeida
Fabrício Vasconcelos Gomes
Fernando Issao Ninomiya
Laurianne-Marie Schippers
Lívia Pazianotto Torres
Marcelo de Castro Cunha Filho
Maria Cecilia Oliveira Gomes
Marília Papaléo Gagliardi
Jordan Vinícius de Oliveira
Thaís Duarte Zappelini

Pesquisadores responsáveis por este Guia

Fábio Ferraz de Almeida

Sumário

1. CONTEXTUALIZAÇÃO

O presente Guia faz parte da série de documentos da FGV intitulada **"Orientações para a Governança de Dados da FGV"** e tem como objetivo fornecer orientações sobre como gerenciar as diversas atividades e operações de tratamento de dados. Este Guia é um dos frutos do projeto de adequação da FGV em relação a Lei Geral de Proteção de Dados (**LGPD**) e outras leis setoriais sobre o tema.

A Fundação Getulio Vargas consciente da importância e da necessidade de adequar as suas operações de tratamento de dados pessoais a uma nova e ampla regulação sobre o tema, no caso, a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – "**LGPD**"), aprovada em agosto de 2018, deu início em maio de 2019 ao seu processo de conformidade. Considerando ainda, que em maio de 2018 entrou em vigor o *General Data Protection Regulation* (Regulation EU 2016/679 – "**GDPR**") e, que este possui pontos de contato com as atividades da FGV na União Europeia (UE), foi decidido que o processo de conformidade regulatória também abarcaria este regulamento além de outras leis setoriais de proteção de dados brasileiras.

A **LGPD** é uma lei transversal, que perpassa por diferentes agentes econômicos no Brasil, como a academia, setor privado, setor público e terceiro setor. Entre os agentes regulados, a FGV se situa no setor acadêmico como uma Instituição de Ensino Superior (IES), abrangendo por esse motivo, uma série de particularidades nos tratamentos de dados pessoais realizados em sua estrutura. Particularmente, a FGV precisa atender às obrigações legais específicas de IES previstas pelo MEC e outras entidades, as quais muitas vezes possuem sinergia com o campo da proteção de dados, devido a particularidades no tratamento de dados do setor educacional, como por exemplo, a necessidade de guarda permanente de históricos escolares, provas, etc.

Considerando que a FGV é uma IES e, portanto, depositária de um grande volume de dados de caráter pessoal coletados em pesquisas científicas e na administração do ensino, por meio de fontes como cadastros de matrícula, históricos escolares, cadastros de professores e funcionários administrativos, entre outros, decidiu-se pela necessidade de desenvolver um projeto para cumprir com os objetivos de sua conformidade regulatória frente às leis de proteção de dados, denominado **Projeto Presidência - Implantação do Programa de Conformidade: Leis de Proteção de Dados Pessoais ("Projeto")**.

Dessa forma, o Projeto visa, primeiramente, a realizar um levantamento das práticas de tratamento de dados pessoais em toda a FGV. Considerando seu histórico, sua dimensão e suas diferentes frentes de atuação, o Projeto tem o objetivo de viabilizar uma análise completa, levando em consideração as distintas particularidades envolvidas em cada uma das atividades desempenhadas pela FGV. O Projeto tem como objetivo também desenvolver metodologias e mecanismos de análise para elaboração de Relatórios de Impacto à Proteção de Dados que visem a contribuir com a construção de uma cultura de proteção de dados na FGV e nas demais IES no País.

Como resultado desse trabalho, busca-se desenvolver: (i) a conformidade da FGV ao novo contexto regulatório de proteção de dados da **LGPD** e, subsidiariamente, àquele estabelecido pela **GDPR**; e (ii) estabelecer um protocolo de conformidade ao novo marco legal de proteção de dados pessoais em IES, com potencial de disseminação e replicação por outras instituições e de influência de agentes governamentais e outros atores privados.

O processo de conformidade envolve um trabalho de interpretação da lei para definição das obrigações legais, diagnóstico dos fatos pertinentes e relevantes para a sua aplicação e levantamento de fluxos e processos que contribuem ou não para que os fatos estejam de acordo com o documento legal.

2. DEFINIÇÕES

A presente seção trata de conceitos-chave mencionados ao longo deste Guia. Para melhor disposição, os termos foram agrupados de acordo com: (i) conceitos gerais sobre a **LGPD** e sobre temas de Recursos Humanos; (ii) conceitos específicos sobre princípios previstos na **LGPD**; (iii) e conceitos específicos sobre direitos do(a)s titulares consoante a **LGPD**. Todas as definições foram dispostas por ordem alfabética.

2.1. CONCEITOS GERAIS

AGENTE DE TRATAMENTO: o controlador e o operador (Art. 5º, IX, LGPD).

ANONIMIZAÇÃO: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo (Art. 5º, XI, LGPD). O dado anonimizado, nos termos da lei, deixa de ser considerado dado pessoal, garantindo maior liberdade no seu tratamento (Art. 12, LGPD).

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS ("ANPD"): órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da Lei em todo território nacional (Art. 5º, XIX, LGPD). A ANPD foi instituída pela LGPD como órgão da administração pública federal com autonomia técnica, integrante da Presidência da República, definida sua natureza como transitória e passível de transformação pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República (Art. 55-A).

BASE LEGAL: trata-se do fundamento que autoriza o tratamento de dados pessoais por um agente, devendo ser definida, em casos concretos, a partir de uma das hipóteses dispostas na LGPD ao seu artigo 7º (caso de dados pessoais) ou ao seu artigo 11 (caso de dados pessoais sensíveis). As bases legais só não serão necessárias nos casos em que a LGPD não se aplica, como nas hipóteses do artigo 4º ou em situações de processamento que envolvam dados anonimizados, onde a identificação da

titularidade não seja possível por meios razoáveis.

CONSENTIMENTO: manifestação livre, informada e inequívoca (Art. 7º, I, LGPD) pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada (Art. 5º, XII, LGPD). Deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular (Art. 8º, LGPD).

CONTROLADOR: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (Art. 5º, VI, LGPD). É quem determina como os dados são processados.

CRIANÇA: pessoa até doze anos de idade incompletos (Art. 2º do ECA).

DADO PESSOAL: informação relacionada a pessoa natural identificada ou identificável (Art. 5º, I, LGPD). Também são considerados dados pessoais para os fins da lei aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada (Art. 12, §2º, LGPD).

DADO PESSOAL SENSÍVEL: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (Art. 5º, II, LGPD).

ENCARREGADO *(DATA PROTECTION OFFICER - "DPO"):* é a pessoa física ou jurídica indicada pelo Agente de Tratamento para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

***GDPR* (*GENERAL DATA PROTECTION REGULATION*):** Regulamento Geral sobre a Proteção de Dados 2016/679. Trata-se de regras relativas à proteção das pessoas naturais no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Revogou a Diretiva 95/46 /CE (Regulamento Geral de Proteção de Dados).

LGPD (LEI GERAL DE PROTEÇÃO DE DADOS): Lei 13.709/2018 dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado (Art. 1º, LGPD). Aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que: (i) a operação de tratamento seja realizada no território nacional; (ii) a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou (iii) os dados pessoais objeto do tratamento tenham sido coletados no território nacional (Art. 3º, caput e incisos I a III, LGPD).

OPERADOR: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (Art. 5º, VII, LGPD). É quem acata as ordens de como os dados devem ser processados.

ÓRGÃO DE PESQUISA: é o órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional, em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico (Art. 5º, XVIII, da LGPD).

ÓRGÃO/DEPARTAMENTO/UNIDADE DE RH: todo órgão, departamento ou unidade que desempenha, mesmo que secundariamente, função de gestão de RH, ainda que de maneira secundária ou episódica. Essa função é verificada no exercício das tarefas relacionadas à seleção, contratação, pagamento, acompanhamento durante a vigência da prestação de serviço, e desligamento de funcionários/ associados/ colaboradores.

TITULAR: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento (Art. 5º, V, LGPD).

TRATAMENTO: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (Art. 5º, X, LGPD).

TRANSFERÊNCIA INTERNACIONAL DE DADOS: é a transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro (Art. 5º, XV, LGPD).

UNIÃO EUROPEIA ("UE"): é um bloco econômico composto por 28 países da Europa (27 com o Brexit, isto é, com a saída do Reino Unido), sendo eles: Áustria, Bélgica, Bulgária, Croácia, Chipre, República Checa, Dinamarca, Estônia, Finlândia, França, Alemanha, Grécia, Hungria, Irlanda, Itália, Letônia, Lituânia, Luxemburgo, Malta, Holanda, Polônia, Portugal, Romênia, Eslováquia, Eslovênia, Espanha, Suécia, Reino Unido.

2.2. PRINCÍPIOS DA LGPD

Na terminologia jurídica, um princípio é um tipo de norma que deve ser cumprida na maior medida possível e cujo conteúdo serve como diretriz geral de interpretação para situações concretas. Na **LGPD**, os princípios estão listados ao longo do artigo 6° e são os seguintes:

ADEQUAÇÃO: compatibilidade do tratamento com as **finalidades** informadas ao titular, de acordo com o contexto do tratamento (art. 6º, II, **LGPD**).

BOA-FÉ: significa a observância de um comportamento leal, correto e probo na realização das atividades de tratamento de dados pessoais. Esse princípio, opera como norte a todos os demais e servindo de baliza para interpretar conceitos abertos (art. 6º, caput, **LGPD**).

FINALIDADE: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível ou desvirtuada (art. 6º, I, **LGPD**).

LIVRE ACESSO: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais (art. 6º, IV, **LGPD**).

NÃO DISCRIMINÇÃO: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos (art. 6º, IX, **LGPD**).

NECESSIDADE: limitação ou minimização do tratamento ao mínimo necessário para a realização de suas **finalidades**, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às **finalidades** do tratamento de dados (art. 6º, III, **LGPD**).

PREVENÇÃO: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais (art. 6º, VIII, **LGPD**).

QUALIDADE DOS DADOS: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento (art. 6º, V, **LGPD**).

RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas (art. 6º, X, **LGPD**).

SEGURANÇA: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão (art. 6º, VII, **LGPD**).

TRANSPARÊNCIA: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial (art. 6º, VI, **LGPD**).

2.3. DIREITOS DO TITULAR NA LGPD

Os direitos dos titulares de dados estão previstos majoritariamente ao longo do artigo 18 da LGPD. Ademais, há ainda o direito de titularidade (artigo 17) e, com relação a tratamentos automatizados, os direitos de informação e de revisão (artigo 20):

ACESSO AOS DADOS: o titular de dados tem resguardado o seu interesse de receber uma cópia dos dados pessoais detidos pela empresa, se assim o requisitar (art. 18, II, LGPD). Conforme a LGPD, tal direito será objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências (art. 13, § 3º, LGPD). Sublinha-se que os órgãos notariais e de registro devem fornecer acesso aos dados por meio eletrônico para a

administração pública, tendo em vista as suas finalidades (art. 23, § 5º, LGPD).

ANONIMIZAÇÃO, BLOQUEIO OU ELIMINAÇÃO: o titular de dados tem o direito de solicitar que seus dados sejam anonimizados, bloqueados ou que haja a eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei (art. 18, IV, LGPD).

CONFIRMAÇÃO DA EXISTÊNCIA DE TRATAMENTO: direito do titular a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição de informações sobre a existência de tratamento (art. 18, I, LGPD), isto é, de toda operação realizada com seus dados pessoais (art. 5º, X, LGPD).

CORREÇÃO DE DADOS INCOMPLETOS, INEXATOS OU DESATUALIZADOS: o titular de dados pode requerer a retificação dos dados, caso estejam incorretos, insuficientes, imprecisos, não expressem a completude das informações armazenadas ou careçam de atualização (art. 18, III, LGPD).

ELIMINAÇÃO DOS DADOS PESSOAIS: o titular de dados pode requerer que seus dados sejam excluídos, de forma que a empresa deverá eliminar todos os dados coletados com relação a esse titular, a não ser que exista outra base legal para a manutenção desses dados (art. 18, VI, LGPD).

INFORMAÇÃO SOBRE COMPARTILHAMENTO: o titular de dados pode solicitar informações das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados (art. 18, VII, LGPD).

INFORMAÇÃO SOBRE O NÃO CONSENTIMENTO: o titular de dados pode solicitar informações sobre a possibilidade e hipóteses de não fornecimento do consentimento, além de entender sobre as consequências da negativa (art. 18, VIII, LGPD).

INFORMAÇÃO SOBRE TRATAMENTO AUTOMATIZADO: o titular de dados pode pedir informações a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada. Tais informações, a serem oferecidas pelo controlador, deverão apresentar clareza e adequação com o que foi solicitado (art. 20, §1º, LGPD).

OPOSIÇÃO: o titular de dados pode se opor ao contexto do tratamento de dados e/ou às finalidades do tratamento, incluindo tratamento realizado com fundamento em uma das hipóteses de dispensa do consentimento (art. 18, §2º, LGPD).

PETIÇÃO: o titular de dados pode fazer qualquer requerimento com relação aos seus dados contra o controlador perante a autoridade nacional (art. 18, §1º, LGPD).

PORTABILIDADE: disponibilização dos dados do titular a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador (art. 18, V, LGPD).

REVISÃO: o titular de dados pode pedir revisão das decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões

destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (art. 20, caput, LGPD).

REVOGAÇÃO DO CONSENTIMENTO: manifestação expressa do titular, por procedimento gratuito e facilitado (art. 18, IX, LGPD), ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação (art. 8º, §5º, LGPD).

TITULARIDADE DOS DADOS PESSOAIS: a toda pessoa natural é assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade (art. 17, LGPD), de modo que o titular é, portanto, a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento (art. 5º, V, LGPD).

3. ESCOPO DE APLICAÇÃO

Este Guia estabelece orientações e recomendações para resguardo e utilização segura de dados pessoais que venham a ser tratados nas atividades de pesquisa realizadas por órgãos de pesquisa. A principal referência legal utilizada para sua elaboração foi a LGPD, embora outras normas nacionais e internacionais também tenham sido consideradas, com especial atenção ao *General Data Protection Regulation* ("GDPR"), o Regulamento Geral sobre Proteção de Dados Pessoais da União Europeia.

4. OBJETIVOS

São objetivos do Guia de Proteção de Dados: Pesquisa:

(a) Apresentar aos pesquisadores as disposições estabelecidas pela legislação que tratam de proteção de dados pessoais na pesquisa;

(b) Estabelecer diretrizes e orientações aos pesquisadores, que assegurem e reforcem o compromisso que todo órgão de pesquisa deve ter com o cumprimento das legislações de proteção de dados pessoais aplicáveis; e

(c) Orientar a condução das atividades e operações de tratamento de dados pessoais realizadas pelos destinatários deste Guia no âmbito de pesquisa, de forma a garantir a sua conformidade com as legislações de proteção de dados pessoais, em especial com a LGPD.

Os demais documentos da FGV que se relacionam com este Guia são:

(i) Política de Privacidade e Proteção de Dados Pessoais FGV;

(ii) Manual de Procedimentos: Ética em Pesquisa.

5. PROTEÇÃO DE DADOS PESSOAIS E PESQUISA

O processo de *Compliance* envolve trabalho de interpretação jurídica para definição das obrigações legais, diagnóstico dos fatos pertinentes e relevantes para a sua aplicação, e levantamento de fluxos e processos que contribuem ou não para que os fatos estejam de acordo com o documento legal.

Para o *European Data Protection Supervisor* (EDPS)[1], braço da União Europeia de supervisão do cumprimento das regras de proteção aos dados pessoais, a pesquisa científica cumpre função muito importante em sociedades democráticas: a construção de novas formas de conhecimento e a busca por sociedades mais desenvolvidas e justas. Neste contexto, a coleta, análise, compartilhamento e armazenamento de informações são operações fundamentais para a realização da atividade científica. Dados, portanto, estão no centro da atividade de pesquisadores e de órgãos de pesquisa.

No cenário europeu, o EDPS descreve que o regime europeu de proteção de dados pessoais criou uma estrutura flexível de aplicação das normas de proteção de dados pessoais, reduzindo o ônus do setor para a sua adequação em razão dos benefícios que a atividade oferece para os países membros da entidade. **A flexibilização das regras busca desfazer a ideia de que o regime de proteção aos dados pessoais poderia servir como um obstáculo ao progresso da ciência**. Na visão do EDPS, na sociedade da informação é natural que a pesquisa científica incorpore preocupações em relação ao tratamento de dados pessoais da mesma forma que que o setor desenvolveu preocupações éticas na condução de estudos, em especial com seres humanos.

Não há no regime jurídico europeu uma definição formal e universalmente aceita de pesquisa científica. Da mesma forma, a legislação brasileira de proteção de dados pessoais utiliza as expressões "pesquisa", "atividade de pesquisa" e "atividades acadêmicas" sem defini-las. O EDPS, no entanto, enfatiza que há parâmetros para a identificação de atividades que devam ser tratadas como atividades de pesquisa. Na visão da entidade, a pesquisa se apresenta como uma **atividade sistemática** realizada por pesquisador ou órgão de pesquisa que será realizada a partir de **um método reconhecido pela comunidade científica** para orientar a investigação e **disponibilizará publicamente os seus resultados** para o progresso do conhecimento humano.

Para o EDPS, a proteção de dados pessoais não deve obstaculizar que chamou de "expressão acadêmica do pesquisador", que se manifesta em três dimensões: (i) liberdade do pesquisador em

[1] Em 06 de janeiro de 2020, o *European Data Protection Supervisor* (EDPS) publicou um relatório chamado de "A Preliminary Opinion on Data Protection and Scientific Research" tratando da aplicação do "General Data Protection Regulation" (GDPR) para a atividade de pesquisa científica no âmbito da jurisdição dos países membros da União Europeia. O documento é uma referência importante para a aplicação de normas presentes no contexto europeu para as atividades de pesquisa científica em diversas áreas, tendo uma atenção especial para a área de estudos em saúde (e.g. testes clínicos e laboratoriais). Para mais informações sobre o relatório, consulte:<https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf>.

tratar de dados pessoais para a disseminação do resultado de pesquisas; (ii) fazê-lo por meio de publicações de resultados em periódicos, sem restrições, sendo preservada a transparência e o acesso aos dados; e (iii) o compartilhamento de metodologias de pesquisa e critérios de análise de dados com seus pares, podendo trocar visões e opiniões sobre os mais diferentes temas.

A preocupação com a proteção de dados pessoais em atividades de pesquisa, surge sobretudo no contexto de projetos que contam com apoio de empresas, públicas ou privadas, e busca evitar o reaproveitamento de dados pessoais para desenvolvimento de atividades comerciais no ambiente corporativo. A flexibilização das regras de proteção de dados pessoais aplicadas para a área de pesquisa não deve ser apropriada pelo setor corporativo, não podendo isentar empresas de cumprir com suas obrigações de proteção de dados pessoais.

No Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD) compartilha da mesma preocupação europeia. Diferente de outros setores, a área de pesquisa recebeu um tratamento flexível na LGPD, semelhante ao contexto europeu. A partir das definições de órgão de pesquisa e tratamento de dados para atividades de pesquisa, a LGPD facilitou o uso de dados pessoais para o setor.

Desta forma, os projetos de pesquisa que envolvam informações relativas a pessoas naturais localizadas no Brasil se submetem às regras presentes na LGPD. Quando os dados se referirem a pessoas naturais localizadas fora do território nacional, será aplicada a LGPD e, ainda, a regra do país em que estejam localizadas. No caso de pesquisas realizadas em parceria com instituições europeias ou que envolvam dados de pessoas em território europeu (restrito aos países da União Europeia) a regra será o GDPR e as legislações nacionais cabíveis. **Mesmo em um regime flexível, regras sobre transparência, segurança da informação e as condições para o exercício de direitos por titulares de dados pessoais devem ser observadas por órgãos de pesquisa**.

Por esta razão, o propósito deste Guia é apresentar as disposições estabelecidas pela legislação que trata de proteção de dados pessoais em pesquisa. Este documento serve como orientação geral para os pesquisadores.

Antes de prosseguir com o conteúdo do Guia, contudo, cabe um aviso. A matéria da proteção de dados pessoais ainda é nova, e traz diversas controvérsias e incertezas sobre as regras aplicáveis, especialmente no caso da atividade de pesquisa. O próprio EDPS, em determinados momentos, aponta para a existência de inúmeros desafios da regulação nessa temática. O presente Guia, inclusive, está baseado em interpretação da LGPD construída em parte de maneira original pela FGV a partir do estudo de referências internacionais e nacionais (extremamente escassas) e reflexão sobre o tema. Assim, é natural que muitas dúvidas apareçam na condução de atividades de pesquisa. As soluções para tais dúvidas deverão ser construídas em conjunto entre os usuários do Guia e as instâncias competentes do Órgão de Pesquisa, como seu Comitê de Ética e seu Encarregado de Proteção de Dados Pessoais.

RESUMO: INTRODUÇÃO À PROTEÇÃO DE DADOS E PESQUISA

- Para o ***European Data Protection Supervisor*** **(EDPS)** a "expressão acadêmica do pesquisador", manifesta-se: (i) na liberdade em tratar de dados pessoais para a disseminação do resultado de pesquisas; (ii) em publicações de resultados em periódicos, sem restrições, sendo preservada a transparência e o acesso aos dados; e (iii) no compartilhamento de metodologias de pesquisa e critérios de análise de dados com seus pares, podendo trocar visões e opiniões sobre os mais diferentes temas;
- **No Brasil**, os projetos de pesquisa que envolvam informações relativas a pessoas naturais localizadas no Brasil se submetem às regras presentes na LGPD.
- **Regras sobre transparência, segurança da informação e as condições para o exercício de direitos** por titulares de dados pessoais devem ser observadas por **órgãos de pesquisa.**

5.1 O QUE É PROTEÇÃO DE DADOS PESSOAIS?

Segundo Lothar Determann[2], a proteção de dados pessoais visa ao resguardo das informações que dizem respeito a pessoas naturais. O foco não é o indivíduo, mas sim o dado e as consequências que o seu uso indevido pode trazer para as pessoas naturais. Compreender o regime de proteção de dados pessoais criado na Europa, que influenciou diversas jurisdições, incluindo a brasileira, é entender que este regime está centrado na lógica geral presente no termo "verboten", significando "proibido" em tradução do alemão. Empresas e organizações que tratam dados pessoais estão como regra geral proibidas de fazê-lo a não ser que apresentem **salvaguardas ao titular**, como a obtenção de seu consentimento válido (base legal para o tratamento), sejam transparentes em relação aos seus usos e compartilhamentos (transparência), mantenham-se subordinadas ao escopo de finalidades apresentadas (princípio da finalidade), dentre outras obrigações.

[2] Lothar Determann é sócio do escritório de advocacia Baker & Mackenzie e Professor associado da Universidade Livre de Berlim, Universidade da Califórnia e Escola de Direito da Universidade Berkeley. Coordenou projetos de conformidade em proteção de dados pessoais no Vale do Silício para empresas e Universidades, bem como participou de forma ativa em projetos de conformidade em proteção de dados pessoais no continente europeu, O seu Guia de Conformidade é uma referência na área de privacidade e proteção de dados pessoais, sendo utilizado por diversos projetos pelo mundo, em especial no contexto de Compliance corporativo. Para mais informações, consulte: DETERMANN, Lothar. Guia de Campo de Determann sobre o Direito à Privacidade de Dados: Compliance Corporativo Internacional. 4ª edição. Rio de Janeiro: Lumen Juris, 2019.

Na área de pesquisa científica, flexibiliza-se o número de salvaguardas a serem apresentadas pelo Órgão de Pesquisa que irá tratar dados pessoais, valorizando-se os benefícios trazidos no âmbito das atividades que favorecem o progresso da ciência. Todavia, segundo Lothar Determann[3], a flexibilização do número de salvaguardas para a área de pesquisa não deve ser confundida com a possibilidade de tratar livremente dados pessoais acessíveis publicamente. **Dados pessoais de acesso público recebem a mesma proteção do que os dados pessoais não disponíveis publicamente**. **O que define a proteção conferida é o caráter pessoal do dado e não onde e de que forma é oferecido**. A legislação brasileira caminha no mesmo sentido, não diferenciando de que forma o dado pode ser obtido, mas sim qual a natureza do dado, pessoal ou não pessoal. Assim, a título de exemplo, o uso dos dados pessoais disponibilizados em sites governamentais cujo acesso é público também se submete à LGPD.

Neste sentido, a proteção de dados pessoais no Brasil busca equilibrar os interesses de privacidade das pessoas naturais e as necessidades das organizações de fazer uso justo e razoável das informações dessas pessoas. Isto não significa que pesquisadores não possam utilizar informações desse tipo, nem que necessitem sempre obter o consentimento para tal uso. A legislação apenas impõe controles e restrições aos quais os pesquisadores devem se conformar.

ATENÇÃO! DADOS PESSOAIS DE ACESSO PÚBLICO

Dados **pessoais de acesso público** recebem a mesma proteção do que os dados pessoais não disponíveis publicamente. O que define a proteção conferida é o caráter pessoal do dado e não onde e de que forma é oferecido.

5.2 POR QUE A PROTEÇÃO DE DADOS PESSOAIS É IMPORTANTE PARA A PESQUISA?

No diagnóstico do EDPS, o processo de digitalização dos dados transformou a pesquisa científica. Os custos da coleta e do armazenamento de dados têm caído ao longo dos últimos anos, ao passo que a capacidade de processamento de dispositivos eletrônicos que auxiliam na análise de dados tem aumentado. Pesquisadores, em especial do campo da saúde, buscam por mais dados e dependem destes para ampliar suas descobertas em seus campos de conhecimento. Redes de pesquisa colaborativas se formaram ao longo dos últimos anos para ampliar o potencial de descobertas científicas a partir da concentração de mentes privilegiadas que enfrentariam

[3] DETERMANN, Lothar. Guia de Campo de Determann sobre o Direito à Privacidade de Dados: Compliance Corporativo Internacional. 4ª edição. Rio de Janeiro: Lumen Juris, 2019, p. 5.

em conjunto problemas complexos. Neste cenário, o uso e o compartilhamento de dados são inevitáveis e, na visão do EDPS, fundamentais para o progresso da ciência.

Um dos principais desafios descritos pelo EDPS para a proteção de dados pessoais em atividades de pesquisa científica é a relação entre órgãos de pesquisa e empresas (privadas e públicas) participantes dos projetos. Isto porque, em alguns projetos de pesquisa, pode haver **compartilhamento de dados pessoais** entre o órgão de pesquisa e a empresa participante, dificultando o controle das finalidades do tratamento de dados pessoais, bem como o exercício de direitos pelo titular de dados pessoais. Além disso, o EDPS aponta preocupações com o número crescente de casos em que violações de normas de proteção de dados pessoais tiveram início em pesquisas iniciadas em universidades.

Como exemplo de violações decorrentes de pesquisa, cabe citar o caso da Cambridge Analytics. Em apertada síntese, conforme a investigação do *Information Commissioner's Office* (ICO)[4], autoridade de proteção de dados pessoais britânica, os primeiros experimentos de análise de dados e formação de perfis comportamentais na rede social Facebook tiveram início no Centro de Pesquisa em Psicometria da Universidade de Cambridge, Reino Unido. A infraestrutura técnica desenvolvida no Centro de Pesquisa (e.g. softwares, algoritmos de coleta e análise de dados, metodologias de classificação etc.) estabeleceu as bases para a criação da empresa Cambridge Analytics, envolvida na coleta ilícita de dados pessoais na rede social e no uso não autorizado de dados pessoais de usuários do Facebook. Parte dos pesquisadores que desenvolveram a infraestrutura técnica da pesquisa do Centro de Pesquisa foram também os fundadores da empresa, tendo as investigações do ICO demonstrado que estes pesquisadores faziam coletas de dados e testes com os dados para a construção de perfis comportamentais que não respeitavam as regras europeias de proteção dados pessoais.

Outro exemplo citado pelo EDPS é o de formação de redes de pesquisa entre empresas, universidades e governo. Em 2015, a Google celebrou com o *National Health Service* (NHS), sistema público de saúde do Reino Unido, um acordo de cooperação para pesquisa para a análise de dados pessoais sensíveis de 1,6 milhões de pacientes que passaram pelo sistema. No acordo, centros de pesquisa universitários ligados ao NHS iriam se utilizar de uma infraestrutura de análise de dados oferecida pela *DeepMind*, empresa controlada pela Google, para a realização de estudos em diversas áreas (e.g. HIV, doenças mentais, doenças auto-imunes, etc.). O acordo foi objeto de investigação por parte da autoridade britânica de proteção de dados pessoais, pois a Google e a NHS não obtiveram o consentimento específico dos pacientes envolvidos nas pesquisas. Segundo a Conselheira Elizabeth Dunham do ICO, mesmo que as pesquisas tivessem um potencial de trazer grandes benefícios para a sociedade, os pacientes têm o direito de saber e autorizar o uso de seus dados pessoais, especialmente seus dados pessoais sensíveis (e.g. informações sobre sua saúde).

Os dois exemplos descritos pelo EDPS revelam preocupações concretas para a área de pesquisa

[4] A autoridade britânica de proteção de dados pessoais preparou um relatório com a descrição do escopo da investigação, documentos analisados e o resumo de sua decisão. Para detalhes sobre o caso, consulte: < https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf>.

no tema proteção de dados pessoais. Os casos apresentados servem como ilustrações de preocupações para a conformidade realizada no Brasil a partir da LGPD. Mesmo que não se tenha uma equivalência entre as normas europeias e brasileiras, há paralelos relevantes que podem ser construídos a partir da experiência no contexto europeu.

Por esta razão, a conformidade das atividades de pesquisa à LGPD e às demais leis setoriais que tratam de proteção de dados pessoais é fundamental. O descumprimento dos dispositivos previstos na LGPD pode resultar em uma série de sanções administrativas estabelecidas pela lei (e.g. advertências e multas) e condenações cíveis, além de prejudicar a reputação do órgão de pesquisa.

Todo órgão de pesquisa deve estar compromissado com o tratamento responsável de informações relativas às pessoas naturais e com o respeito aos direitos de privacidade e de proteção de dados pessoais destes indivíduos. Embora as considerações sobre a legislação de proteção de dados possam parecer um fardo adicional para os pesquisadores, grande parte das orientações e cuidados aqui previstos são práticas comuns da pesquisa e, regra geral, consistentes com as recomendações feitas pelos comitês de ética ou integridade dos órgãos de pesquisa.

RESUMO: IMPORTÂNCIA DA PROTEÇÃO DE DADOS PARA PESQUISA

- Em alguns projetos de pesquisa, pode haver **compartilhamento de dados pessoais** entre o órgão de pesquisa e a empresa participante, dificultando o controle das finalidades do tratamento de dados pessoais, bem como o exercício de direitos pelo titular de dados pessoais;
- O descumprimento das previsões legais pode resultar em uma série de sanções administrativas estabelecidas pela lei e condenações cíveis, além de **prejudicar a reputação do órgão de pesquisa.**

5.3 QUAIS OS PRINCÍPIOS QUE DEVEM PAUTAR O TRATAMENTO DE DADOS PESSOAIS NO ÂMBITO DA PESQUISA?

Os pesquisadores devem pautar o tratamento de dados pessoais no âmbito da pesquisa nos princípios elencados pela LGPD, quais sejam:

(a) Finalidade;
(b) Adequação;
(c) Necessidade;
(d) Livre acesso;
(e) Qualidade dos dados;
(f) Transparência;
(g) Segurança;
(h) Prevenção;
(i) Não discriminação
(j) Responsabilização e prestação de contas.

Embora vários dos princípios elencados acima sejam autoexplicativos, é importante comentá-los especificamente no contexto da realização de pesquisa.

a) Finalidade

Este princípio estabelece que se determinado dado pessoal foi obtido para uma finalidade específica, seu uso não deve ser permitido para outras finalidades que sejam incompatíveis com o propósito original. No caso de atividade de pesquisa, entretanto, entende-se que é possível a **reutilização de dados pessoais** originalmente coletados para outras finalidades, porém permanece o dever do pesquisador de **informar os titulares** de dados pessoais afetados. Esta prática de reutilização é por vezes chamada de tratamento secundário de dados pessoais, em que informações que identificam um indivíduo são coletadas em um contexto distinto do da atividade de pesquisa, mas são reaproveitados por pesquisadores. O cuidado aqui é com a comunicação com o titular de dados pessoais, ele tem de ter as condições de saber quem está tratando os seus dados e para quais propósitos, em cumprimento ao princípio da transparência, discutido abaixo.

DEFINIÇÃO

Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível ou desvirtuada.

Vale ressaltar que a autorização de reutilização de dados pessoais é **exclusiva** para a área de pesquisa, não podendo ser estendida para outras atividades distintas, como por exemplo, para o aprimoramento de produtos e serviços de empresas. Isto significa que os dados utilizados no âmbito de uma pesquisa não poderão ser reaproveitados comercialmente, salvo se a empresa obtiver a autorização necessária para a realização do tratamento destes dados pessoais. Esta é uma das dimensões do regime flexível da proteção de dados pessoais para as atividades de pesquisa.

A apresentação da finalidade em uma pesquisa que trata dados pessoais precisa estar enunciada do projeto até a publicação dos seus resultados. A finalidade pode ser apresentada na metodologia do estudo, em seus objetivos ou nas justificativas da pesquisa. Não há nenhuma proibição para que um acréscimo seja incluído dispondo de uma nova finalidade ao estudo, bem como para a realização de mudanças durante a execução das operações de tratamento. Contudo, na ocorrência de acréscimos, supressões e/ou mudanças nas finalidades presentes na condução do estudo, o pesquisador terá de informar o titular de dados pessoais de todas as mudanças realizadas na medida que forem implementadas na pesquisa.

Considerando que em muitos momentos é impossível para o pesquisador antecipar com absoluta precisão a maneira pelo qual serão utilizados os dados (e.g. pesquisas de cunho exploratório) e que é normal haver ajustes metodológicos no curso de determinadas pesquisas a partir dos dados encontrados, a necessidade de estabelecer uma finalidade específica é interpretada com flexibilidade para a área de pesquisa, sendo tolerável a definição de finalidades mais amplas, contanto que justificadas com base no tipo de pesquisa realizada. As mudanças e especificações, contudo, devem ser registradas e comunicadas tão logo aconteçam.

b) Adequação

Este princípio está conectado ao anterior e existe para garantir a **compatibilidade** entre a **finalidade informada** ao titular do dado pessoal e a **efetiva prática de tratamento** de dados colocado em curso pelo agente de tratamento. Para fins desse princípio, considera-se que a pesquisa é finalidade compatível com todas as finalidades pelas quais os dados foram originalmente coletados.

DEFINIÇÃO

Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

Um exemplo recente discutido no contexto europeu e que auxilia na compreensão do princípio da adequação é o de serviços de testagem genética. Empresas provedoras destes serviços (e.g. 23 and Me) têm compartilhado dados coletados no âmbito de suas relações com seus clientes com centros de pesquisa em universidades na Europa. A finalidade principal do serviço é a coleta de dados genéticos para a oferta de informações sobre ancestralidade e genes associados a enfermidades. Os clientes da empresa enviam uma amostra de saliva para a empresa que extrai o DNA da amostra, classifica as informações genéticas e as apresenta por meio de suas plataformas digitais (e.g. aplicativo, site etc.). Segundo o EDPS, é muito comum que empresas provedoras deste serviço não informem seus clientes que estão compartilhando os dados genéticos com centros de pesquisa universitários. Mesmo que a finalidade de realização de pesquisa com dados genéticos para o combate de doenças seja adequada, a não comunicação do compartilhamento torna o tratamento destes dados ilegítimo, por violação do princípio da transparência. Por esta razão, centros de pesquisa em universidades europeias têm solicitado a confirmação de que o compartilhamento dos dados foi comunicado aos titulares de dados pessoais.

c) Necessidade

Este princípio é chamado na Europa de princípio da minimização. Ele revela uma das preocupações centrais da proteção de dados pessoais, a utilização excessiva de dados pessoais de titulares. Por esta razão, o princípio estabelece que o tratamento de dados pessoais deve se limitar a **quantidade de dados mínima necessária** para a realização de finalidades pré-estabelecidas e informadas ao titular de dados pessoais. O objetivo desse princípio é prevenir a realização de uma coleta de dados pessoais desnecessários, criando riscos injustificados ao titular.

DEFINIÇÃO

Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

Cabe aqui a mesma observação realizada acima sobre a impossibilidade de antecipar com absoluta precisão quais serão os dados necessários e seus usos em determinados tipos de

pesquisa. O princípio da necessidade não visa a proibir ou obstaculizar pesquisas de cunho exploratório, busca apenas evidenciar alguns nexos causais entre a atividade de pesquisa e as operações de tratamento de dados pessoais realizadas. Na prática, isto significa que cabe ao pesquisador responsável por uma pesquisa de natureza exploratória o registro das suas atividades de pesquisa, descrevendo quais dados pessoais foram coletados, como eles podem contribuir para o seu objeto de pesquisa e de que forma foram utilizados, prevendo inclusive o seu descarte quando não forem necessários para a sequência do estudo. Ressalte-se que estes cuidados já são observados na postura de pesquisadores como boas práticas, tendo agora de ser observados por força de lei.

Importante ressaltar que o princípio se aplica também aos demais tratamentos realizados com a finalidade de pesquisa e não apenas à quantidade e às espécies de dados coletados. Por exemplo, em alguns projetos pode não ser necessário que todos os membros da equipe de pesquisa ou colaboradores externos tenha acesso à base de dados completa, sendo possível providenciar a esses indivíduos acesso aos dados em sua forma anonimizada ou pseudonimizada. Os pesquisadores devem sempre considerar se existe de fato uma necessidade de usar dados pessoais ou se seria possível atingir os objetivos da pesquisa por meio de dados anonimizados, agregados ou pseudonimizados.

d) Livre acesso

Este princípio propõe-se a garantir aos titulares dos dados pessoais utilizados em pesquisa a **consulta facilitada e gratuita** sobre como e até quando esses dados serão tratados, bem como sobre a integralidade dos dados usados.

DEFINIÇÃO

Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.

A garantia do livre acesso se vincula aos direitos do titular, os quais também são de certo modo relaxados no caso da atividade pesquisa. A esse respeito, confira a seção 16 deste Guia.

e) Qualidade dos dados

É importante que os pesquisadores garantam aos titulares que seus dados sejam exatos, claros,

relevantes e atualizados na medida do possível, considerando o cumprimento da finalidade de seu tratamento, no caso, a de pesquisa.

DEFINIÇÃO

Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados pessoais, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

A garantia de qualidade dos dados não permite que um titular solicite a alteração dos dados coletados, caso isso interfira na metodologia da pesquisa. Trata-se de outro princípio vinculado aos direitos do titular, os quais também são de certo modo relaxados no caso da atividade pesquisa. A esse respeito, confira a seção 16 deste Guia.

f) Transparência

Este princípio refere-se ao oferecimento de **informações claras, precisas e acessíveis** aos titulares dos dados com relação ao uso dos dados pessoais e seu eventual compartilhamento com outros agentes de tratamento. No caso da pesquisa, é importante que os pesquisadores informem aos titulares dos dados, por exemplo, com quem essas informações são compartilhadas (e.g. outros pesquisadores da equipe, colaboradores externos, etc.).

O cuidado aqui é garantir as condições de rastreabilidade dos dados pessoais utilizados por parte de seu titular. Nesse sentido, recomenda-se que projetos de pesquisa sejam capazes de informar o titular de dados pessoais sobre os seguintes aspectos envolvendo o tratamento: (i) tipo de dados utilizados (e.g. CPF, nome, etc.); (ii) finalidades do tratamento; (iii) se o tratamento é primário (coleta direta pelo pesquisador) ou secundário (reutilização de dados coletados por terceiro); (iv) quem terá acesso aos dados (e.g. lista dos pesquisadores e terceiros com os quais os dados sejam compartilhados para fins da execução da pesquisa); (v) tempo de armazenamento dos dados; e (vi) canal de comunicação com a equipe de pesquisa; (vii) canal de consulta dos dados do titular.

O dever de transparência é um dos mais relevantes na intersecção entre pesquisa e proteção de dados pessoais. A valorização atribuída para a descrição detalhada e específica sobre todas as etapas e procedimentos realizados no âmbito de uma atividade de pesquisa passa a ser exigida no contexto da proteção de dados pessoais, em particular no tratamento de dados pessoais sensíveis. A recomendação é que a prestação de informações se inicie no projeto e acompanhe

os pesquisadores na apresentação de seus resultados. Um alto padrão de transparência já conferia à pesquisa maior credibilidade em relação aos seus resultados, com a LGPD passa a também atribuir maior proteção aos titulares que contribuíram para o estudo com seus dados pessoais.

DEFINIÇÃO

Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial tratamento.

Embora seja possível, em tese, imaginar um conflito entre transparência e ineditismo ou originalidade de uma pesquisa, isto é pouco provável na prática. A chave para evitar o conflito está no **nível de detalhamento** necessário por parte do pesquisador. A apresentação de informações sobre as atividades da pesquisa e sua metodologia é fundamental, contudo, a descrição de cada etapa não precisa ser exaustiva.

Transparência não significa a descrição detalhada da metodologia de pesquisa enquanto a pesquisa está sendo desenvolvida. Isto porque: (i) em alguns casos não é possível, pois a pesquisa pode sofrer transformações a partir de suas primeiras etapas e dos dados coletados; e (ii) há pesquisas que, pelas suas próprias características, como pesquisas exploratórias, as definições se darão durante a sua execução.

Por fim, interessante assinalar que um dos limites para o dever de transparência reconhecido pela LGPD é o segredo comercial e industrial. Protege-se a possibilidade de resguardo da confidencialidade sobre um produto ou serviço de modo a garantir a proteção de ativos intelectuais. Nesse sentido, a transparência deve se dar em relação aos dados brutos, coletados para fins da realização da pesquisa. As inferências, análises, e construções com base nos dados pessoais é passível de confidencialidade até o término da pesquisa e sua publicação.

g) Segurança

O princípio da segurança cria a obrigação ao pesquisador e ao órgão de pesquisa de demonstrar a adoção de medidas técnicas e organizacionais para a prevenção de incidentes de segurança, especialmente de acessos não autorizados aos dados pessoais de titulares. Os cuidados a serem tomados não se limitam ao âmbito digital, de adoção de medidas no contexto da tecnologia da informação (e.g. firewall), mas estendem-se também para o contexto físico, em que documentos

com informações pessoais também devem ser guardados de modo a prevenir acessos não autorizados (e.g. não se deve deixar documentos com informações sensíveis de titulares sobre a mesa de espaço coletivo de trabalho). O acesso não autorizado é particularmente preocupante, pois pode levar ao uso indevido de dados pessoais, seja em formato digital ou físico. Por esta razão, o princípio da segurança cria a obrigação ao pesquisador e ao órgão de pesquisa que ele representa o dever de apresentar garantias de segurança da concepção do projeto até a apresentação de seus resultados, estendendo-se também estas obrigações para a hipótese que a guarda dos dados pessoais seja necessária para preservação de uma série histórica de informações.

Falhas de segurança da informação podem causar sérios danos e prejuízos aos indivíduos aos quais os dados pertencem. O princípio da segurança determina que os pesquisadores tomem as medidas técnicas e organizacionais para proteger os dados pessoais de acessos não autorizados, ataques e acidentes de tratamento. Essas medidas devem procurar garantir, por exemplo, que: (i) apenas pessoas autorizadas possam acessar, alterar, divulgar ou eliminar dados pessoais; (ii) essas pessoas ajam apenas dentro do seu escopo específico na pesquisa; (iii) na eventualidade de perda acidental de dados pessoais, estes possam ser recuperados para evitar qualquer dano ou prejuízo aos titulares dos dados.

DEFINIÇÃO

Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Uma recomendação comum é o controle de acessos aos dados pessoais por meio de um *logbook* ou outra ferramenta similar. A rastreabilidade de quem teve acesso e quando teve acesso é uma forma de redução do risco de acessos não autorizados. Além disso, uma vez que este acesso não autorizado ocorra, esta ferramenta também pode servir como instrumento de verificação e esclarecimento do incidente de segurança.

Em termos práticos, recomenda-se que no tratamento de dados pessoais em atividades de pesquisa sejam utilizados: (i) sistema de autenticação de usuários com acesso aos dados pessoais (verificação da identidade do pesquisador, por exemplo, por e-mail institucional); (ii) compromisso do pesquisador na adoção de senhas fortes (e.g. número mínimo de caracteres, mistura de letras e números, não referência a nomes e datas de cunho pessoal, etc.); (iii) autenticação por dois fatores (duas senhas distintas); (iv) estrutura de controle de acesso aos

dados pessoais (predefinição dos usuários com privilégios de acesso); e (v) uso preferencial de criptografia na guarda de dados em dispositivos eletrônicos.

Não há solução única para todos os problemas referentes à segurança de informação na pesquisa, tampouco há solução que sirva para sempre, diante da evolução da tecnologia da informação. Recomenda-se que os pesquisadores, periodicamente e em conjunto com a área de tecnologia de informação do órgão de pesquisa, considerem os avanços tecnológicos em segurança e a viabilidade para a implementação dessas tecnologias. O nível de segurança adotado em um projeto de pesquisa deverá ser compatível com os riscos envolvidos no projeto (e.g. pesquisas que envolvam dados pessoais sensíveis deverão adotar medidas mais rigorosas).

Além disso, é necessária a diferenciação entre as atividades de pesquisa realizadas por pesquisadores individuais (e.g. programas de pós-graduação) das realizadas por centros, núcleos, grupos e institutos de pesquisa. Mesmo que as recomendações sejam as mesmas, observa-se que a capacidade de implementação do pesquisador individual será mais limitada do que a de entes de pesquisa que realizam a atividade de forma contínua e profissional. Por esta razão, recomenda-se que pesquisador individual entre em contato com o responsável assinalado pelo órgão de pesquisa quando tiver dúvidas sobre a adoção de medidas de segurança para a sua pesquisa.

Para a gestão dos dados pessoais em meio físico (e.g. documentos) a orientação é a guarda dos dados em locais com acesso restrito (e.g. armários com sistema de trava por chave) e a adoção de máquinas fragmentadoras de papel. O descarte de documentos com a presença de dados pessoais (e.g. jogar um contrato no lixo comum) representa um risco de segurança para o titular de dados pessoais, em especial quando há dados pessoais sensíveis envolvidos. O recolhimento de documentos com dados pessoais no lixo, por exemplo, pode ser caracterizado como um acesso não autorizado da mesma forma que a invasão de uma plataforma digital. Por esta razão, ressaltamos a importância de uma boa administração de documentos na condução de pesquisas.

Em resumo, a segurança física dos dados pessoais inclui fatores como o acesso ao local onde os dados estão armazenados, eliminação de material impresso e a segurança de equipamentos portáteis como laptops e tablets. Recomenda-se, na medida do possível, que o acesso e o armazenamento dos dados pessoais sejam feitos nos computadores do órgão de pesquisa ao qual o pesquisador é vinculado.

h) Prevenção

Este princípio está intimamente conectado ao princípio da segurança e busca garantir a adoção de medidas capazes de prevenir a ocorrência de danos em virtude do tratamento de dados pessoais. Este princípio exige uma postura proativa do pesquisador, um cuidado no registro das operações de tratamento realizadas, a descrição das medidas de segurança adotadas para os dados pessoais tratados no âmbito da pesquisa, um cuidado na administração de senhas de acesso e no compartilhamento de dados com outros pesquisadores e com terceiros.

Uma prática comum na área de pesquisa é a criação de senhas consideradas fracas para permitir o acesso à bancos de dados com informações de indivíduos. A respeito desta prática, a

Commission Nationale L'IInformatique et des Liberté (CNIL), autoridade francesa de proteção de dados pessoais, produziu um relatório[5] com um conjunto de recomendações que buscam reduzir os riscos envolvendo a criação e a gestão de senhas. A caracterização de uma senha como fraca é apontada como um risco de segurança para a administração do acesso às informações de cunho pessoal. A adoção de medidas que busquem reduzir os riscos da adoção de senhas fracas é encarada como prevenção à potenciais incidentes de segurança no contexto de operações de tratamento de dados pessoais.

Para a CNIL, em processos de autenticação da identidade de um pesquisador baseada apenas em uma etapa de verificação (e.g. solicitação de apenas uma senha para acesso aos dados), a senha deve conter, no mínimo, 12 caracteres, caso contrário será considerada fraca. A senha deve conter letras maiúsculas e minúsculas, números e, se possível, não deve fazer qualquer alusão a informações de cunho pessoal. A recomendação da autoridade francesa é que os responsáveis pelo tratamento, em nosso caso, coordenadores de pesquisa ou orientadores de trabalho devem informar seus pesquisadores e orientandos, respectivamente, dos riscos da adoção de senhas fracas para a pesquisa, para a instituição de pesquisa e para os titulares de dados pessoais.

Para os casos em que a autenticação da identidade é feita por mais de um fator de autenticação, o número de caracteres mínimos pode ser reduzido. São exemplos disso, autenticação por uma senha e restrição no acesso a determinadas informações, por exemplo, limitando o acesso de pesquisadores apenas a parcelas do conjunto de dados pessoais armazenados. A CNIL estabelece que uma senha terá que conter, no mínimo, 8 caracteres para não ser considerada fraca. Da mesma forma, se além da senha, for solicitada, por exemplo, a confirmação de uma informação adicional, e.g. sobrenome da mãe do pesquisador, a CNIL recomenda que a senha tenha, no mínimo, 5 caracteres.

DEFINIÇÃO

Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

[5] O relatório produzido pela autoridade francesa de proteção de dados pessoais busca apresentar um conjunto de recomendações para a administração de senhas por parte de indivíduos, definindo os riscos de senhas fracas e do compartilhamento de senhas entre pessoas. Para mais informações sobre o documento, consulte: <https://www.cnil.fr/sites/default/files/atoms/files/recommandation_passwords_en.pdf>.

Estes exemplos servem para ilustrar o tipo de postura preventiva esperada por parte de pesquisadores e órgãos de pesquisa. É natural que órgãos de pesquisa criem seus protocolos internos de segurança, prevendo a obrigatoriedade de atualizações periódicas de senhas, número mínimo de caracteres, autenticações em mais de uma etapa, dentre outras determinações. Há um espaço razoável de liberdade para a escolha das medidas de segurança por órgãos de pesquisa e por pesquisadores, permitindo com que as regras para o setor sejam distintas de órgão para órgão. O que não muda, entretanto, é a obrigatoriedade de adoção pelo pesquisador e pelo órgão de pesquisa de medidas que comprovem uma postura preventiva.

i) Não discriminação

Ao tratar dados pessoais, os pesquisadores devem considerar como esses dados afetam ou podem afetar os interesses dos seus titulares, ficando proibida a realização de tratamentos que possuam finalidades discriminatórias, ilícitas ou abusivas.

DEFINIÇÃO

Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

Recomenda-se que os comitês de ética ou integridade do órgão de pesquisa ao qual o pesquisador está filiado sejam envolvidos na verificação do atendimento ao princípio da não-discriminação.

j) Responsabilização e prestação de contas

O princípio da responsabilização e prestação de contas é uma tradução do *accountability principle*, presente em outras jurisdições. Este princípio busca permitir que operações de tratamento de dados pessoais possam ser auditadas, mesmo depois do encerramento da pesquisa. A conservação da memória das operações realizadas e suas finalidades é parte integrante do princípio da responsabilização e prestação de contas. Os pesquisadores e os órgãos de pesquisa devem ser capazes de explicar quais operações foram realizadas e seus propósitos, mesmo após o término da pesquisa.

A LGPD introduziu esse princípio na legislação brasileira, de modo que os agentes de tratamento, no caso, os órgãos de pesquisa, devem ser capazes de demonstrar a adoção de medidas que comprovem a conformidade de suas atividades às normas reguladoras de proteção de dados,

inclusive os princípios aqui elencados. É fundamental, portanto, que sejam documentadas quaisquer políticas e procedimentos adotados pelos pesquisadores e órgãos de pesquisa para se conformar aos requisitos estabelecidos pela legislação sobre proteção de dados pessoais. Parte desse esforço consiste em manter algum tipo de registro das atividades de tratamento dos dados pessoais no contexto da pesquisa (e.g. coleta, acesso, compartilhamento, eliminação etc.).

DEFINIÇÃO

Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Recomenda-se que esses registros contenham, por exemplo, as categorias de titulares de dados (de quem os dados foram coletados), as categorias de dados pessoais (quais tipos de dados foram coletados), as categorias dos recipientes (com quem os dados são compartilhados, caso o sejam), detalhes referentes à transferência internacional (com quais países e instituições é feito essa transferência), além de detalhes sobre o prazo de eliminação e uma descrição das medidas de segurança implementadas para realizar a pesquisa.

Recomenda-se que o pesquisador ou a unidade de pesquisa (e.g. centro, núcleo, grupo) seja o ponto de registro das informações sobre tratamento de dados pessoais no âmbito de suas pesquisas específicas e compartilhem essas informações com as instâncias competentes dos órgãos de pesquisa ao qual estejam vinculados (e.g. por meio de formulários, relatórios de atividades etc.). A prestação de esclarecimentos sobre as operações de tratamento de dados pessoais às autoridades públicas, deverá ser feita por intermédio do encarregado do órgão de pesquisa.

6. QUAL A POSIÇÃO DO ÓRGÃO DE PESQUISA EM PROJETOS DE PESQUISA E SUAS RESPONSABILIDADES?

O órgão de pesquisa pode ocupar diferentes posições quanto ao tratamento de dados pessoais: (i) **controlador**: responsável pelas decisões referentes ao tratamento de dados pessoais nos projetos de pesquisa; (ii) **co-controlador**: arranjos de controle conjunto com divisão de responsabilidades para a estruturação de projetos de pesquisa; e (iii) **operador:** executor das

operações de tratamento de dados pessoais a partir de instruções lícitas do controlador, retendo autonomia técnica.

A definição da posição ocupada pelos agentes de tratamento nem sempre é tarefa fácil, especialmente diante da vagueza do conceito de autonomia técnica. Nos casos em que houver dúvida sobre a posição ocupada pelo órgão de pesquisa em determinado projeto, recomenda-se a consulta ao encarregado da instituição. Contudo, algumas regras gerais podem ser apresentadas que auxiliam a indicar a provável posição ocupada pelo órgão de pesquisa:

- Quando há **autonomia acadêmica**, e o pesquisador vinculado ao órgão de pesquisa decide a forma de tratamento dos dados pessoais, o órgão assume a posição de **controlador**;

- Quando o órgão de pesquisa é contratado para realizar alguma **tarefa específica** no âmbito de um projeto maior, devendo seguir instruções dos responsáveis pelo projeto original a respeito do tratamento, o órgão de pesquisa contratado será um **operador** ou **co-controlador**, a depender do **grau de liberdade e autonomia** concedido. Quanto mais participação houver na definição geral do uso dos dados e da metodologia, estabelecimento dos resultados almejados, e na realização de inferências, a tendência é que haja co-**controle**.

Em relação às responsabilidades, na posição de **controlador**, o órgão de pesquisa tem a **obrigação de reparação** em caso de dano gerado a outrem decorrente de violação à legislação de proteção de dados pessoais no exercício de suas atividades. Na hipótese de **controle compartilhado** das decisões sobre o tratamento de dados pessoais, o órgão de pesquisa responde pelas operações em que estejam **diretamente envolvido**. No caso em que ocupa a posição de **operador**, o órgão de pesquisa é responsável quando (a) **não seguir instruções lícitas** do controlador; e (b) **descumprir as regras da LGPD** (nesse caso, a responsabilidade é tanto do controlador quanto do operador).

O **controlador** possui, ainda, a responsabilidade de atender às solicitações realizadas com base nos direitos dos titulares. A esse respeito, confira a seção 16 deste Guia. Por fim, cumpre elencar ainda que a Autoridade Nacional de Proteção de Dados Pessoais (ANPD) publicou o seu Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado[6], o qual traz alguns critérios sobre a definição do papel dos agentes de tratamento.

[6] Ver especialmente conteúdo contido no intervalo das páginas 07-21: https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/2021-05-27-guia-agentes-de-tratamento_final.pdf.

DEFINIÇÃO

Órgão de pesquisa: *"órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico"* (Art. 5º, XVIII, da LGPD).

RESUMO: POSIÇÃO DO ÓRGÃO DE PESQUISA

- O órgão de pesquisa poderá, na qualidade de **agente de tratamento**, ser controlador (toma as decisões sobre o tratamento de dados pessoais), operador (acata as ordens do controlador) ou, ainda co-controlador (age em conjunto com um segundo controlador);
- Quando há **autonomia acadêmica**, e o pesquisador vinculado ao órgão de pesquisa decide a forma de tratamento dos dados pessoais, o órgão assume a posição de **controlador**;
- Quando o órgão de pesquisa é contratado para realizar **tarefa específica** no âmbito de um projeto maior, devendo seguir instruções dos responsáveis pelo projeto original a respeito do tratamento, o órgão de pesquisa contratado será um **operador ou co-controlador, a depender do grau de liberdade e autonomia concedido.**
- Em caso de dúvidas remanescentes, ver o **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado**, da ANPD, disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/2021-05-27-guia-agentes-de-tratamento_final.pdf.

7. SUA PESQUISA ENVOLVE TRATAMENTO DE DADOS PESSOAIS?

A LGPD aplica-se apenas ao **tratamento** de **dados pessoais**. Regra geral, será fácil identificar se o seu projeto de pesquisa entra no escopo da lei, mas isso pode não ser sempre o caso, daí a importância de consideramos os elementos constitutivos abaixo.

Tratamento é definido pela LGPD como toda operação realizada com dados pessoais, incluindo a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Note-se que são muitas operações abrangidas pelo termo 'tratamento'. Explica-se: se um pesquisador recebe um banco de dados com informações pessoais (e.g. nome, CPF, endereço, etc.), a operação de tratamento 'recepção' de dados pessoais foi realizada e a LGPD incide sobre esta operação, antes mesmo de qualquer análise do banco de dados. Da mesma forma, na hipótese de acesso remoto às bases de dados administradas por outras universidades, por exemplo no *Harvard Library Bibliographic Data se*t, o acesso aos dados, sua visualização, caracteriza-se como a operação de tratamento 'acesso', podendo, se houver qualquer tipo de interação com os dados (e.g. inserção, modificação), a operação ser classificada ainda como outro tipo de tratamento de dados pessoais. Neste sentido, é muito difícil imaginar operações envolvendo dados pessoais que não sejam classificadas como tratamento.

DEFINIÇÃO

O que é **tratamento**?

Toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

A principal dúvida, portanto, passa ser a de identificar se os dados tratados no âmbito de determinada pesquisa podem ser classificados como pessoais. Na definição da LGPD, dados pessoais são as informações relacionadas à pessoa natural identificada ou identificável. Dados identificados são aqueles em que a capacidade de identificação de um indivíduo deriva do próprio dado. Um exemplo disso é o número do cadastro de pessoas físicas, o CPF, em que a uma sequência numérica identifica

apenas um cidadão brasileiro. Em posse deste número uma pessoa é capaz de alcançar o titular do CPF.

O tipo de acesso ao dado, se público ou privado, não influencia na classificação de uma informação como dado pessoal. Por esta razão, informações disponibilizadas em bases de dados públicas recebem nível de proteção idêntico ao das informações presentes em bases de dados privadas, tendo o seu tratamento de respeitar as mesmas normas presentes na LGPD. Uma pesquisa que coleta, classifica, transmite e armazena dados pessoais disponíveis publicamente, por exemplo em plataformas digitais do governo federal (e.g. consumidor.br) deve respeitar as mesmas regras de transparência e segurança do que as que são objeto das mesmas operações de tratamento em bases de dados de acesso privado.

A maior dificuldade envolvendo o conceito de dados pessoais são os dados identificáveis, também chamados de dados de identificação indireta, isto é, aqueles que, em si, não permitem a identificação de um indivíduo, mas em conjunto com outros dados em um contexto específico podem ter como resultado do seu tratamento a identificação de uma pessoa natural.

A autoridade britânica de proteção de dados pessoais (ICO)[7], apresenta um exemplo interessante de combinação de dados não pessoais que podem gerar a identificação de pessoas. A ICO cita que a idade, a profissão e o endereço, individualmente, não são encarados como dados pessoais, contudo, em um mesmo banco de dados podem identificar uma pessoa natural. Tome o exemplo da ICO, de uma pessoa com 34 anos, bióloga e residente na rua X, cidade Y. As chances de que existam mais de uma pessoa com esta combinação são muito reduzidas, tornando a identificação desta pessoa quase uma certeza. Vale notar que a possibilidade de identificação é uma questão de grau. Se há grandes chances de haver identificação de uma pessoa em razão da maneira pela qual os dados estão organizados, eles devem ser considerados dados de uma pessoa identificável, atraindo a aplicação das regras sobre proteção de dados pessoais.

Uma questão muito comum sobre a identificação indireta diz respeito a seu limite, pois em última instância, todo dado poderia ser considerado como pessoal por identificação indireta. A ICO aponta para três fatores que devem ser levados em consideração: (i) tempo exigido para a identificação; (ii) custo exigido para a identificação; e (iii) tecnologia disponível para o cruzamento de dados não pessoais no momento do tratamento, considerando desenvolvimentos tecnológicos recentes. Se o tempo e custo para a identificação forem altos e a tecnologia a ser empregada for sofisticada e custosa, mesmo que seja possível a identificação indireta, os dados não devem ser considerados pessoais.

É fato que estes parâmetros ainda assim são demasiadamente amplos. Por esta razão, cabe ao pesquisador e ao órgão de pesquisa avaliarem o objeto da pesquisa, seus objetivos e as características gerais das bases de dados a serem utilizadas. Recomenda-se que o pesquisador entre em contato

[7] A Information Commissioner's Office (ICO) apresenta em seu site oficial um conjunto amplo de explicações sobre a aplicação de regras sobre proteção de dados pessoais. Em uma destas páginas de explicação, a autoridade britânica explica como pode se dar a identificação indireta de pessoas naturais a partir do uso conjunto de dados não pessoais em determinados contextos. Para mais informações, consulte: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/can-we-identify-an-individual-indirectly/>.

com a instância competente do órgão de pesquisa, em caso de dúvida.

ATENÇÃO! COMO IDENTIFICAR DADOS PESSOAIS?

Se há grandes chances de haver **identificação de uma pessoa** em razão da maneira pela qual os dados estão organizados, eles devem ser considerados **dados de uma pessoa identificável**, atraindo a aplicação das regras sobre proteção de dados pessoais. Cabe considerar: (i) tempo exigido para a identificação; (ii) custo exigido para a identificação; e (iii) tecnologia disponível para o cruzamento de dados não pessoais no momento do tratamento, considerando desenvolvimentos tecnológicos recentes.

7.1 É NECESSÁRIO CONSENTIMENTO PARA REALIZAR ATIVIDADES DE PESQUISA?

Não, a LGPD não exige o consentimento do titular para a realização de estudos promovidos por órgão de pesquisa (nos termos dos Arts. 7º, IV e 11, II, c) da LGPD), ressaltando a necessidade de anonimização dos dados pessoais sempre que possível (vide Seção 9.2, abaixo)[8].

Discute-se no Brasil se a obtenção de consentimento não deveria ser obrigatória para o pesquisador em atividades de pesquisa que apresentam questões éticas relevantes, como por exemplo estudos na área genética. Apesar de a discussão ser importante, ela extrapola a proteção de dados pessoais. **O consentimento para os fins de atendimentos às normas éticas não se confunde com o consentimento para fins de proteção de dados pessoais. É plenamente possível que o consentimento seja dispensável do ponto de vista da proteção de dados pessoais e necessário do ponto de vista ético**. Se houver coleta de consentimento por razões éticas, isso não significa que o tratamento de dados pessoais tenha que ser baseado necessariamente em consentimento. Com efeito, a base legal do consentimento é inconveniente para a pesquisa pelo regime jurídico que atrai, especialmente pela possibilidade de o titular poder revogar o seu consentimento a qualquer tempo, o que poderia dificultar a execução da pesquisa ou alterar seus resultados.

8 Diferentemente da LGPD, a GDPR não possui uma base legal para tratamento específica para a pesquisa. No entanto, isso não significa que o consentimento seja sempre necessário no tratamento de dados pessoais com a finalidade de pesquisa, ainda que seja necessário em razão de alguma norma ética. Os dois consentimentos não se confundem. Assim, a GDPR a princípio também admite o tratamento de dados pessoais para pesquisa sem consentimento, mas deve haver cuidados próprios na justificação. Nesse sentido, a autoridade britânica, ICO em "What are the rules on consent for scientific research purposes?", disponível em https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/#what10 .

Pela definição da lei, órgãos de pesquisa são as entidades (públicas ou privadas) que não possuem finalidade lucrativa e têm como missão institucional a pesquisa básica ou aplicada, histórica, científica, tecnológica ou estatística. Contudo, se alguma entidade é definida como órgão de pesquisa, isso não significa que a posição efetivamente assumida pela entidade será sempre a de órgão de pesquisa. Por exemplo, um Centro, Núcleo, Grupo ou Instituto vinculado a um órgão de pesquisa pode ser contratado para a realização de atividades de consultoria, em cenários nos quais bancos de dados com dados pessoais forem compartilhados com empresas (públicas ou privadas), em um escopo de trabalho pré-definido e cujos resultados não sejam disponibilizados publicamente. Nesses casos a atividade realizada não é de pesquisa e, portanto, as obrigações incidentes sobre a entidade serão as mesmas aplicáveis às empresas.

Nesse sentido, uma preocupação apresentada pelo EDPS é o do **reaproveitamento comercial** de dados pessoais por empresas em sua relação com órgãos de pesquisa. A flexibilização do regime de proteção de dados pessoais aplicada ao setor de pesquisa está diretamente relacionada aos benefícios que o setor traz para a sociedade. Por esta razão, a área de pesquisa não deve ser usada como um meio para o não cumprimento das obrigações incidentes sobre o setor empresarial. O cuidado aqui é avaliar o **escopo** da parceria (e.g. consultoria) entre o órgão de pesquisa e as empresas, com foco nas **contrapartidas** solicitadas pelas empresas, em especial se há publicização dos resultados e eventuais solicitações exclusivas aos dados gerados no curso da pesquisa. A questão é complexa e a recomendação é que cada parceria seja analisada caso a caso pela instância competente do órgão de pesquisa, a fim de oferecer parecer sobre a posição do órgão no caso, bem como esclarecer as salvaguardas para os titulares decorrentes do projeto de pesquisa.

Outro cuidado importante para ser tomado aqui são as parcerias realizadas pelo órgão de pesquisa com universidades europeias. No cenário europeu, a dispensa do consentimento do titular para fins da realização da pesquisa é mais restrita, cabendo cuidado especial na definição da base legal para tratamento de dados pessoais. Mesmo que no Brasil a LGPD não requeira a obtenção do consentimento do titular, na hipótese de pesquisas conjuntas com universidades europeias, com o tratamento de dados pessoais de parte a parte, recomenda-se que o órgão de pesquisa siga o mesmo protocolo de obtenção de consentimento da universidade estrangeira parceira, caso exista.

ATENÇÃO! QUANDO A OBTENÇÃO DO CONSENTIMENTO É NECESSÁRIA?

- Em regra, a LGPD não exige o consentimento do titular para a realização de estudos promovidos por órgão de pesquisa (nos termos dos Arts. 7º, IV e 11, II, c) da LGPD), ressaltando a necessidade de anonimização dos dados pessoais sempre que possível;
- **Cuidado com o reaproveitamento comercial** de dados pessoais por empresas em sua relação com órgãos de pesquisa, a área de pesquisa não deve ser usada como um meio para o não cumprimento das obrigações incidentes sobre o setor empresarial;
- Com relação às **Parcerias com instituições estrangeiras**, mesmo que no Brasil a LGPD não requeira a obtenção do consentimento do titular, na hipótese de pesquisas conjuntas com universidades europeias, por exemplo, com o tratamento de dados pessoais de parte a parte, recomenda-se que o órgão de pesquisa siga o mesmo protocolo de obtenção de consentimento da universidade estrangeira parceira, caso exista.

7.2 DADOS ANONIMIZADOS

A capacidade de identificar o indivíduo ao qual a informação se refere é fundamental para a definição de dado pessoal. Quando o indivíduo não puder ser identificado a partir de determinada informação, esta não será considerada dado pessoal e os deveres e obrigações estabelecidos pela LGPD não se aplicarão a esse caso. A anonimização de dados é, em si, uma forma de proteção ao indivíduo, um resguardo em relação à sua exposição. Não por acaso, a LGPD em diversas disposições recomenda a anonimização como uma das medidas protetivas ao titular de dados pessoais, uma vez que na hipótese de um incidente envolvendo dados anonimizados (e.g. vazamento), os prejuízos serão praticamente nulos ao indivíduo. A lógica presente na lei é: **pesquisador, quando possível, anonimize os dados pessoais objeto de sua pesquisa**.

A escolha de uma técnica de anonimização para a base de dados tratada pela pesquisa não é uma tarefa simples. Há uma pluralidade de técnicas disponíveis (e.g. *noise addition*, *permutation*, *differential privacy*, *aggregation*, *K-anonymity*, *L-diversity*, *T-closeness*, dentre outras), cada uma

delas com virtudes e defeitos[9]. O pesquisador pode não conhecer as diferenças entre cada uma delas para tomar uma decisão informada. Por essa razão, recomendamos que, quando necessário, a área de tecnologia de informação ou outra instância competente com o conhecimento técnico necessário, pertencente ao órgão de pesquisa, seja consultada para ajudar o pesquisador na escolha. Para auxiliá-los, há três perguntas relevantes a serem feitas para a identificação da qualidade de uma técnica de anonimização:

(i) Risco de Reidentificação: A técnica sugerida impede, salvo esforços significativos de tempo e custo, a identificação de um indivíduo pelo dado anonimizado?

(ii) Risco de Inferência: A técnica sugerida impede a extração de inferências a partir do dado anonimizado que facilitariam a identificação do titular?

(iii) Risco de Composição de Atributos: O banco de dados com informações anonimizadas interage com outros bancos de dados com informações não anonimizadas, permitindo a identificação indireta?

A tabela abaixo foi retirada do parecer técnico do *Article 29 Data Protection Working Party*[10] e contém sugestões de técnicas para desidentificação dos dados pessoais, lembrando sempre que a escolha deve ser feita levando em conta as características da pesquisa:

Técnica	A reidentificação ainda é um risco?	A inferência de dados ainda é um risco?	A possibilidade de composição de atributos do dado ainda é um risco?
Utilização de Pseudônimo	Sim	Sim	Sim
Adição de Ruído	Sim	Talvez não	Talvez não
Substituição	Sim	Sim	Talvez não
Agregação ou k-anonimização	Não	Sim	Sim
l-diversidade	Não	Sim	Talvez não
Privacidade Diferencial	Talvez não	Talvez não	Talvez não

[9] Em caso de dúvidas adicionais sobre as técnicas de anonimização, material adicional recomendado sobre o tema é o "*Guide to Basic Data Anonymisation Techniques*", publicado pela Personal Data Protection Commision – Singapore (disponível em: https://www.pdpc.gov.sg/help-and-resources/2018/01/guide-to-basic-data-anonymisation-techniques). Este documento, inclusive, possui tradução não oficial para a língua portuguesa pelo Gabinete para a Proteção de Dados Pessoais do Governo da Região Administrativa Especial de Macau (disponível em: https://www.gpdp.gov.mo/uploadfile/2019/0417/20190417033911965.pdf).

[10] Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf>

Utilização de hash	Sim	Sim	Talvez não

A anonimização não é o instrumento adequado de proteção para todos os casos, pois há um contingente significativo de atividades de pesquisa em que a identificação é necessária para a obtenção dos resultados almejados. A ICO menciona como exemplo as pesquisas na área de saúde, em que as características individuais do paciente importam para o acompanhamento da evolução de seu estado físico (e.g. testes clínicos). Neste contexto, é importante ressaltar que mesmo que o nome dos pacientes seja substituído em estudos realizados na área de saúde, outras informações do histórico médico, endereço, histórico de doenças de parentes etc. permitem a identificação indireta, o que torna o conjunto de dados utilizados em pesquisa neste exemplo, dados pessoais. Nesse sentido, um cuidado importante para a proteção de dados na área de pesquisa é não adotar a omissão do nome dos participantes de uma pesquisa como ferramenta única de proteção à privacidade do indivíduo.

A tabela a seguir orienta os pesquisadores na escolha da melhor técnica de anonimização, levando em consideração sua familiaridade com esses procedimentos:

Não sei por onde começar	Quando os responsáveis da pesquisa não possuírem nenhuma familiaridade com processos de anonimização, recomenda-se que entrem em contato com a instância competente para verificar os documentos disponíveis sobre o tema e recomendações de técnicas que estarão de acordo com as características da pesquisa.
Conheço, mas tenho dúvidas	Se o pesquisador responsável já tiver familiaridade com técnicas de anonimização, ele poderá tirar dúvidas com a instância competente sobre a escolha entre técnicas. A recomendação mais comum é que a escolha possa observar práticas presentes em outras universidades em pesquisas similares. O padrão de anonimização utilizado por centros de pesquisa em universidades de excelência é um ótimo referencial.
Tenho confiança em minha escolha	A recomendação é o registro da técnica utilizada e a atenção em relação aos acessos e ao armazenamento de dados. Lembrando que uma técnica que hoje é tida como forte, pode não ser considerada forte em alguns anos, por isso é preciso atenção e cuidado na replicação de técnicas utilizadas em pesquisas anteriores.

RESUMO: ANONIMIZAÇÃO

- A anonimização de dados é, em si, uma forma de proteção ao indivíduo, um resguardo em relação à sua exposição;
- Para auxiliá-los, há três perguntas relevantes a serem feitas para a identificação da qualidade de uma técnica de anonimização: (I) Risco de reidentificação; (ii) risco de inferência; e (iii) risco de composição de atributos;
- A anonimização não é o instrumento adequado de proteção para todos os casos, pois há um contingente significativo de atividades de pesquisa em que a identificação é necessária para a obtenção dos resultados almejados.

7.3 DADOS PSEUDONIMIZADOS

Caso a anonimização dos dados pessoais não seja possível nem desejada em função de como afeta os resultados almejados, o pesquisador pode optar pela pseudonimização, tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro. Consiste em substituir um atributo (tipicamente um atributo único) em um registro por outro a fim de dificultar a vinculação de um conjunto de dados com a identidade original de um dado.

Nesse caso, no entanto, o dado pseudonimizado permanece sendo dado pessoal, tendo o pesquisador o dever de se conformar às obrigações legais impostas pela LGPD. Uma espécie de técnica de pseudonimização consiste na substituição do nome de pessoas naturais por um código numérico ou um pseudônimo, como na tabela abaixo:

Antes da Pseudonimização:

Pessoa	Renda Familiar	Orientação Política
José da Silva	R$ 3.500,00	Social Democracia
Marcos Henriques	R$ 7.200,00	Socialismo
Jorge Ferreira	R$ 1.900,00	Capitalismo Autoritário
Jonas Goulart	R$ 12.900,00	Liberalismo

Depois da Pseudonimização:

Código/Pseudônimo	Renda Familiar	Orientação Política
416765	R$ 3.500,00	Social Democracia
324584	R$ 7.200,00	Socialismo
112965	R$ 1.900,00	Capitalismo Autoritário
237908	R$ 12.900,00	Liberalismo

A pseudonimização é facilmente reversível caso o pesquisador guarde, em local seguro, os códigos utilizados, fazendo referência aos dados pessoais originais, como na tabela a seguir:

Código/Pseudônimo	Pessoa
416765	José da Silva
324584	Marcos Henriques
112965	Jorge Ferreira
237908	Jonas Goulart

Portanto, a recomendação é que, sempre que possível e tão logo quanto viável, o pesquisador conserve apenas os dados pseudonimizados, eliminando-se a relação entre os códigos utilizados e o identificador das pessoas.

Diferente da anonimização, a pseudonimização não afasta a aplicação da LGPD nem de qualquer outra norma de proteção de dados pessoais. A pseudonimização é uma técnica que reduz riscos em relação à potenciais incidentes de segurança envolvendo dados pessoais. Um dado pseudonimizado reduz a exposição dos dados pessoais de um titular, uma vez que dificulta o reaproveitamento do dado pessoal em outros contextos. Um cuidado importante é não confundir a aplicação de uma técnica de pseudonimização como se fosse uma técnica de anonimização. Por esta razão, se reforça a recomendação de consulta à instância competente do órgão de pesquisa para o esclarecimento de dúvidas sobre os dois tipos de técnicas.

ATENÇÃO! DADOS PSEUDONIMIZADOS

No caso do **dado** pseudonimizado, ele permanece sendo dado pessoal, tendo o pesquisador o dever de se conformar às obrigações legais impostas pela LGPD. A pseudonimização, contudo, é considerada técnica de segurança da informação desejável sempre que possível para proteger os dados.

7.4 DADOS AGREGADOS

Diversos pesquisadores utilizam-se de dados agregados. A agregação consiste no processo de combinar informações de vários indivíduos em classes, grupos ou categorias mais amplas, de modo que não seja mais possível distinguir as informações relacionadas a cada um desses indivíduos. Nesse caso, esses dados podem deixar de ser considerados pessoais. A capacidade da agregação retirar a pessoalidade do dado, entretanto, dependerá de fatores como o tamanho da população na qual a informação estará ocultada. Mais uma vez, caso haja dúvida se uma agregação afasta o caráter pessoal do dado, recomenda-se de consulta à instância competente do órgão de pesquisa.

7.5 REALIZAÇÃO DE ENTREVISTAS E/OU APLICAÇÃO DE QUESTIONÁRIOS

Ao participar de pesquisas que envolvam entrevistas e/ou aplicação de questionários, há uma dupla preocupação: (i) os indivíduos podem revelar informações que venham a ser consideradas dados pessoais sobre eles próprios ou sobre outras pessoas; (ii) o próprio conteúdo da entrevista ou questionário pode ser considerado um dado pessoal, vez que se trata de uma informação atrelada a uma pessoa.

Diante disso, como regra geral, recomenda-se que o pesquisador, mesmo com o consentimento do participante, utilize técnicas de anonimização ou ao menos de pseudonimização, a fim de que não seja identificado o respondente, nem os dados pessoais sobre ele ou sobre terceiros, excetuando-se o caso no qual o processo de anonimização ou pseudonimização seja incompatível com a metodologia de pesquisa utilizada (e.g. depoimentos orais em entrevistas de história oral).

Vale ressaltar que dependendo do contexto de realização da entrevista ou da aplicação do questionário e dos trechos de entrevista ou de resposta ao questionário disponibilizados, mesmo com a omissão de seu nome, o entrevistado pode ser identificado, às vezes com facilidade, principalmente quando atributos únicos sejam revelados sobre o participante (e.g. seu cargo e empresa, sua voz, sua data de nascimento, entre outros). Em entrevistas realizadas com base em questionários semi-estruturados ou não-estruturados observa-se uma forte tendência de

possibilidade de identificação. A depender das informações divulgadas, o entrevistado pode enfrentar diversos riscos à sua vida pessoal, desde a demissão do trabalho até danos à sua integridade física. Desse modo, recomenda-se, como boa prática, a análise de sensibilidade das informações a partir do contexto, e grande cautela na divulgação. Tal preocupação possui interface com a questão ética, recomendando-se a consulta ao comitê de ética ou integridade de sua instituição para dúvidas e orientações, haja vista a existência de Normas de Ética e Integridade sobre o tema expedidas pelo Conselho Nacional de Saúde (CNS), como a Resolução 510/2016, entre outras.

8. POSSO USAR DADOS SENSÍVEIS EM MINHA PESQUISA?

Sim, não há nenhuma vedação para o tratamento de dados pessoais sensíveis no contexto da realização de atividades de pesquisa. Assim como acontece com os dados pessoais em sentido amplo, o texto da LGPD autoriza a utilização de dados pessoais sensíveis para a realização de estudos por órgãos de pesquisa, dispensando o consentimento, determinando que eles sejam anonimizados sempre que possível.

Um cuidado importante aqui é o **tratamento de dados pessoais de crianças e adolescentes**. Embora não sejam considerados dados pessoais sensíveis, esses dados são regulados de forma diferenciada pela LGPD, **exigindo a obtenção de consentimento específico e em destaque dos pais os responsáveis para o seu tratamento no âmbito de atividades de pesquisa.**

Em relação aos dados pessoais financeiros (e.g. informe de rendimentos), mesmo não sendo eles definidos no Brasil como dados pessoais sensíveis, recomendamos que o seu tratamento seja revestido de igual cuidado e preocupação. No Brasil, há um conjunto de decisões judiciais que tratam da exposição de dados financeiros (e.g. inscrição de consumidor em cadastro de devedores) como violação de direitos constitucionais à privacidade e à intimidade. Por esta razão, nossa recomendação é tratar os dados financeiros como dados pessoais sensíveis nas atividades de pesquisa.

DEFINIÇÃO

Dados pessoais sensíveis: são aqueles que dizem respeito à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Segundo o EDPS, o tratamento de dados pessoais sensíveis merece atenção especial por parte do pesquisador e do órgão de pesquisa. Dados como etnia, vida sexual, saúde, convicção religiosa, dentre outros, têm o potencial de criar cenários de discriminação indevida para o titular. A exposição de dados pessoais sensíveis amplia a vulnerabilidade do titular e pode gerar prejuízos significativos ao indivíduo. Por esta razão, é fundamental que os cuidados com transparência e segurança, mencionados neste guia, sejam observados com maior atenção no tratamento de dados pessoais sensíveis.

Um cuidado importante no tratamento de dados pessoais sensíveis é a construção de inferências a partir de outros dados, pessoais ou não. Registros em vídeo ou imagens, ainda que permitam inferir a etnia dos indivíduos retratados ou a extração de dados biométricos (e.g. máscaras do rosto), não são considerados dados pessoais sensíveis. Todavia, caso sejam inferidos dados biométricos ou étnicos a partir dos vídeos, haverá tratamento de dados pessoais sensíveis. Caso a pesquisa não realize a inferência de dados pessoais sensíveis, mas os dados tratados permitam que essas referências sejam realizadas com facilidade, recomenda-se que os cuidados com segurança adotados sejam os mesmos de dados pessoais sensíveis.

Sendo assim, o cuidado a ser tomado pelo pesquisador é o de identificação dos dados utilizados em sua pesquisa como sensíveis ou não. Em caso de dúvidas, recomendamos a consulta à instância competente do órgão de pesquisa, especialmente ao Encarregado.

ATENÇÃO! USO DE DADOS PESSOAIS SENSÍVEIS

Não há vedação para o tratamento de dados pessoais sensíveis no contexto da realização de atividades de pesquisa. Contudo, requer-se maior cuidado com o tratamento desses dados, visto que podem expor o titular a maiores riscos. Ressalta-se que no caso de dados de **crianças e adolescentes menores de 16 anos**, o tratamento de seus dados sempre requer o consentimento específico e em destaque de pelo menos um de seus pais ou responsáveis.

9. COMO DEVO PROCEDER PARA RECEBER DADOS DE TERCEIROS?

Dados pessoais podem ser recebidos pelo órgão de pesquisa no âmbito de um projeto. Os **cuidados com a recepção** são: (i) registrar quais dados foram recebidos e quem os recebeu; (ii) na ausência de um contrato detalhando o compartilhamento ou a transferência dos dados, solicitar uma declaração do terceiro com relação à conformidade deste com a LGPD; (iii) na hipótese dos dados não estarem anonimizados, ter clareza sobre quais pesquisadores terão acesso aos dados; e (iv) dar publicidade ao projeto, com a divulgação do parceiro que forneceu os dados, bem como das categorias de dados recebidas.

A recomendação padrão para o pesquisador é no sentido de que este prefira receber os dados de forma anonimizada. Não sendo possível recebê-los já **anonimizados**, a orientação é de que proceda à anonimização assim que os receber. No caso de pesquisas em que, em virtude de suas próprias características, a anonimização das informações não seja possível, deve-se redobrar os cuidados com o **armazenamento** dos dados e os controles de acesso.

RESUMO: CUIDADOS COM A RECEPÇÃO DE DADOS EM PESQUISA

- **Registrar** quais dados foram recebidos e quem os recebeu;
- Na ausência de um **contrato** detalhando o compartilhamento ou a transferência dos dados, solicitar uma declaração do terceiro com relação à conformidade deste com a LGPD;
- Na hipótese dos dados **não estarem anonimizados**, ter clareza sobre quais pesquisadores terão acesso aos dados;
- Dar **publicidade ao projeto**, com a divulgação do parceiro que forneceu os dados, bem como das categorias de dados recebidas.

10. POSSO COMPARTILHAR OS DADOS PESSOAIS COM TERCEIROS?

A regra geral da LGPD é de que o compartilhamento de dados pessoais com terceiros depende de consentimento específico para tanto. Contudo, o compartilhamento de dados pessoais **no âmbito da**

realização de atividades de pesquisa com outros pesquisadores participantes da pesquisa é permitido e não exige a obtenção de consentimento do titular de dados pessoais.

O compartilhamento dos dados de pesquisa com **empresas que prestarão serviços acessórios aos pesquisadores** (e.g. armazenamento ou processamento de dados em nuvem; realização de entrevistas e grupos focais), na condição de meros operadores, também é permitido independentemente de consentimento. Nesses casos, é fundamental que os prestadores de serviço sigam as instruções dos pesquisadores sobre como coletar e utilizar os dados, preservando-se sempre a finalidade de realização de estudo por órgão de pesquisa. Ademais, recomenda-se que o pesquisador tome precauções: (i) na escolha da empresa, que deve ser idônea, estar em conformidade com a LGPD e ser capaz de fornecer garantias suficientes e adequadas para a execução da atividade; e (ii) na contratação da empresa, quando deverão ser inseridas cláusulas de proteção de dados, que se recomenda obter com as instâncias competentes do órgão de pesquisa, incluindo, conforme o caso, disposição referente à eliminação dos dados após a conclusão do serviço prestado.

Nos casos de serviços acessórios para os quais não há formalização de contrato, bastará uma declaração simplificada, que se recomenda obter com as instâncias competentes do órgão de pesquisa, a ser assinada pelo profissional que realizará o tratamento dos dados. Por exemplo, no caso de contratação de serviço de transcrição de entrevistas, a declaração deve ser assinada pelo transcritor e conter orientações sobre segurança e eliminação dos dados. A orientação, nesse caso, é de que o profissional, preferencialmente, realize a transcrição sem precisar armazenar os dados pessoais em computador de uso pessoal, e não retenha cópias das transcrições, se estas não estiverem anonimizadas.

Esclarece-se que, no caso de elaboração de artigos ou pesquisas em conjunto com pesquisadores externos à instituição, os autores externos também serão considerados participantes da pesquisa para fins de compartilhamento, dispensando consentimento. No entanto, recomenda-se que assinem Termos de Compromisso, que se recomenda obter com as instâncias competentes do órgão de pesquisa, declarando que tem ciência da LGPD e seguiram todas as regras de proteção de dados do órgão de pesquisa, bem como será necessário que sejam observadas as salvaguardas de segurança cabíveis, evitando-se o trânsito descuidado de bases de dados. No caso de compartilhamento com pesquisadores internacionais, devem ser observadas ainda as regras de transferência internacional (vide Seção 13).

O compartilhamento dos dados pessoais obtidos na atividade de pesquisa com terceiros em quaisquer outras situações dependerá de consentimento específico para tal finalidade. Isto porque, o reaproveitamento comercial de dados pessoais por empresas é considerado uma violação na LGPD e no regime jurídico europeu. Além disso, há uma preocupação importante de desvio de finalidade no tratamento de dados quando o compartilhamento com terceiros não respeita o consentimento do titular, em especial quando os dados são utilizados para modificações em produtos e serviços de empresas (público ou privadas).

Desta forma, a regra geral para o pesquisador ou o órgão de pesquisa é compartilhar os dados pessoais coletados com outros pesquisadores participantes da pesquisa ou prestadores de serviços

relacionados à pesquisa e, com terceiros **apenas** se obtiverem o consentimento específico do titular para este tratamento.

RESUMO: COMPARTILHAMENTO DE DADOS

- O **compartilhamento dos dados pessoais** obtidos na atividade de pesquisa com **terceiros** em quaisquer outras situações dependerá de consentimento específico para tal finalidade;
- O compartilhamento dos dados de pesquisa com empresas que prestarão serviços acessórios aos pesquisadores na condição de meros **operadores** é permitido independentemente de consentimento. Nesses casos, é fundamental que os prestadores de serviço sigam as instruções dos pesquisadores sobre como coletar e utilizar os dados, preservando-se sempre a finalidade de realização de estudo por órgão de pesquisa. o.

11. OS DADOS PESSOAIS PODEM SER TRANSFERIDOS PARA OUTROS PAÍSES?

Órgãos de pesquisa e seus pesquisadores costumam trabalhar diretamente com instituições estrangeiras na realização de pesquisas, podendo estabelecer uma série de relações com outras universidades fora do Brasil. Dentre as relações mais comuns, vale mencionar: (i) realização de pesquisa conjunta com a construção ou a utilização de bases de dados pelos órgãos de pesquisa; (ii) consulta por pesquisador do órgão de pesquisa brasileiro de bases de dados no exterior administrada por universidade estrangeira; e (iii) consulta por pesquisador estrangeiro de bases de dados administradas pelo órgão de pesquisa brasileiro. Em todas estas operações é possível tratar de operações de transferência internacional de dados, em alguns casos de brasileiros (iii), outros de estrangeiros (ii) ou até de ambos (i).

Embora não proíba expressamente a transferência de dados pessoais para outros países, a LGPD estabelece que ela somente é permitida em casos determinados, dentre eles: (a) quando realizada para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto na própria lei; (b) quando o controlador oferecer e comprovar garantias, por

via de cláusulas contratuais, por exemplo, de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na LGPD; (c) quando a Autoridade Nacional de Proteção de Dados (ANPD) autorizar; (d) quando resultado de compromisso assumido em acordo de cooperação internacional; e (e) quando o titular tiver consentido especificamente e em destaque para a transferência internacional.

O cenário mais comum é a previsão de cláusulas contratuais específicas sobre a transferência internacional de dados em acordos celebrados entre o órgão de pesquisa brasileiro e instituições estrangeiras na área de pesquisa. Um convênio, por exemplo, celebrado entre duas ou mais universidades para o desenvolvimento de pesquisas em conjunto pode já conter as regras específicas para o compartilhamento de dados pessoais entre as entidades, os protocolos (e.g. transparência) a serem seguidos e os padrões de segurança da informação a serem observados. A criação destas regras, protocolos e padrões terão de observar os princípios presentes na LGPD, porém, há espaço para negociação dos termos destes acordos.

Na hipótese de um acordo entre o órgão de pesquisa brasileiro e uma universidade estrangeira não dispor de regras sobre a transferência internacional de dados pessoais, o acesso aos dados pessoais administrados pelo órgão brasileiro por pesquisadores da universidade estrangeira poderá ser feito por meio da obtenção de um consentimento específico e em destaque por parte dos titulares de dados pessoais sob posse do órgão brasileiro. A obtenção do consentimento específico e em destaque pode trazer alguns desconfortos para a atividade do pesquisador e dificuldades de gerenciamento, por esta razão se recomenda que as parcerias internacionais já disponham de cláusula específica de transferência internacional de dados pessoais. É preciso reconhecer, contudo, que em alguns casos pode não existir margem para negociação ou inclusão destas cláusulas no acordo.

É importante, portanto, que o pesquisador verifique se a transferência dos dados pessoais para instituições estrangeiras é amparada por uma das hipóteses acima. Alternativamente, o pesquisador pode optar por anonimizar os dados pessoais objetos de transferência internacional, cenário no qual a LGPD não se aplica, devendo apenas se certificar de que as regras próprias do respectivo comitê de ética ou integridade responsável pela pesquisa sejam seguidas.

RESUMO: QUANDO O TRATAMENTO DE DADOS PESSOAIS É LEGÍTIMO?

- **Pergunta 1:** o tratamento é necessário para a realização do objeto pretendido e da sua finalidade correspondente? Há outra maneira de prosseguir sem o tratamento? Em caso negativo, passar às perguntas seguintes.
- **Pergunta 2:** os dados são tratados para finalidades específicas, explícitas e informadas para o(a) titular e o(a) responsável pelo(a) titular?
- **Pergunta 3:** o tratamento tem fundamento em uma base legal válida e adequada?
- **Pergunta 4:** caso a base legal seja o consentimento, a sua obtenção e registro são realizados de forma adequada?

12. QUAIS OS CUIDADOS ESPECIAIS PARA PUBLICAR PESQUISAS COM DADOS PESSOAIS?

A LGPD não prevê restrições explicitas à publicação de resultados de pesquisa no contexto da proteção de dados pessoais, no entanto, a fim de satisfazer os princípios da lei, alguns cuidados devem ser tomados. Primeiramente, em regra **não deve ser disponibilizado para acesso público o banco de dados com informações pessoais identificadas, utilizado pelo pesquisador. Recomenda-se, sempre que possível a adoção de técnica de anonimização ou pseudonimização, ou, ainda, a divulgação apenas de dados agregados**.

Como boa prática, sugere-se a implantação de controle de acesso. Isso porque o acesso público à bancos de dados com informações pessoais pode expor titulares de dados pessoais à usuários que irão utilizar as informações armazenadas para finalidades diversas da pesquisa, violando a sua finalidade original e criando riscos para o titular. A recomendação é que a publicização de bancos de dados seja sempre precedida de consulta à instância competente do órgão de pesquisa.

No caso de estudos de saúde pública, a LGPD impõe restrições de divulgação de bancos de dados com informações pessoais sensíveis. Nestes casos, **é recomendado que os bancos de dados sensíveis tratados por pesquisadores não sejam disponibilizados para o público**, sendo restrito para interações acadêmicas. O cuidado aqui é maior do que em outros contextos, em especial os dados que identifiquem informações sobre doenças e tratamentos médicos.

RESUMO: CUIDADOS COM A PUBLICAÇÃO DE PESQUISA

- **Não deve ser disponibilizado para acesso público** o banco de dados com informações pessoais identificadas, utilizado pelo pesquisador. É válida, inclusive, a implantação de controle de acesso;
- Recomenda-se, sempre que possível a adoção de técnica de **anonimização ou pseudonimização**, ou, ainda, a divulgação apenas de dados agregados;
- Em **estudos de saúde pública**, a LGPD impõe restrições de divulgação de bancos de dados com informações pessoais sensíveis, recomendando-se que os **bancos de dados sensíveis** tratados por pesquisadores **não sejam disponibilizados para o público,** sendo restrito para interações acadêmicas.

13. OS DADOS PESSOAIS DEVEM SER ELIMINADO EM ALGUM MOMENTO?

A LGPD autoriza a conservação dos dados pessoais utilizados para pesquisa, devendo ser, preferencialmente, anonimizados. Caso deseje manter os dados pessoais após a conclusão da pesquisa, o pesquisador deverá especificar quais deles serão mantidos, se serão anonimizados ou não, e justificar as suas opções, principalmente se não desejar anonimizar.

Nem todos os dados pessoais, entretanto, precisam ser preservados. Desta forma, o pesquisador deve, em primeiro lugar, selecionar os dados que passarão por processo de gestão de longo prazo. Em geral, todo produto que se configure como dado de pesquisa que tenha exigido tempo e muitos recursos para ser obtido deve ser preservado. Qualquer dado que não pode ser facilmente substituído deve ser preservado.

A preservação de determinados dados pessoais após o término da pesquisa para a qual estes foram utilizados justifica-se também pela possibilidade de replicação do estudo (e de sua metodologia) por outros pesquisadores. No armazenamento desses dados deverá o pesquisador tomar as devidas

precauções para evitar incidentes de segurança e.g. implementando controle de acesso ao material. Na impossibilidade de anonimização dos dados, recomenda-se que estes sejam ao menos pseudonimizados.

RESUMO: ELIMINAÇÃO DOS DADOS

- A LGPD autoriza a conservação dos dados pessoais utilizados para pesquisa, devendo ser, **preferencialmente, anonimizados;**
- Caso deseje manter os dados pessoais **após a conclusão da pesquisa**, o pesquisador deverá **especificar quais deles** serão mantidos, se serão anonimizados ou não, e **justificar as suas opções**, principalmente se não desejar anonimizar.

14. O QUE O TITULAR DE DADOS PODE SOLICITAR?

O texto da LGPD assegura uma série de direitos dos titulares dos dados pessoais. No âmbito de atividades dos pesquisadores, o exercício desses direitos deve ser interpretado de modo a não aumentar em excesso os custos da atividade de pesquisa e prejudicar o desenvolvimento científico no Brasil. A tabela abaixo orienta os pesquisadores sobre como atender os pedidos dos titulares dos dados pessoais:

TITULAR PODE SOLICITAR	AVALIAÇÃO CASO A CASO	NÃO APLICÁVEL
▪ Confirmação da existência de tratamento de dados pessoais	▪ Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD	▪ Portabilidade de dados pessoais (não se aplica para atividades de pesquisa)

▪ Acesso aos dados pessoais: apenas brutos e não às inferências e análises sobre os dados pessoais no transcorrer da pesquisa	▪ Revogação do consentimento e eliminação de dados pessoais, aplicáveis quando o tratamento para fins de pesquisa tiver sido realizado com base em consentimento	
▪ Publicação de informações sobre o compartilhamento ou recepção de dados de terceiros (e.g. websites)	▪ Correção de dados incompletos, inexatos ou desatualizados	
	▪ Revisão de tratamento automatizado de dados pessoais	

A confirmação da existência de tratamento e o acesso aos dados pessoais podem ser simplificados, a fim de evitar a criação de uma estrutura excessivamente custosa para fins da realização da pesquisa e desproporcional em relação aos recursos para sua realização. Para fins da definição da estrutura de atendimento recomenda-se a consulta às instâncias competentes do órgão de pesquisa e, conforme a complexidade do caso, ao Encarregado.

15. O QUE NÃO DEVO FAZER AO REALIZAR UMA PESQUISA COM DADOS PESSOAIS?

Ao utilizar dados pessoais no âmbito de sua pesquisa, o pesquisador deve preocupar-se em **não realizar as seguintes condutas:**

	**ATENÇÃO!** **CONDUTAS NÃO RECOMENDADAS** ▪ Reaproveitamento corporativo; ▪ Retenção injustificada; ▪ Recepção sem verificação; ▪ Compartilhamento indevido; ▪ Acessos não-autorizados; ▪ Anonimização fraca; ▪ Eliminação inefetiva; e ▪ Recusa injustificada para solicitação de titulares.

16. ORIENTAÇÕES ESPECÍFICAS

16.1 PESQUISA COM DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES: CUIDADOS ESPECIAIS NA COLETA, ARMAZENAMENTO E ELIMINAÇÃO

Crianças e adolescentes necessitam de proteção especial na coleta e no tratamento de seus dados pessoais por possuírem, na maioria dos casos, menor consciência sobre os riscos envolvidos nessas atividades. No caso de pesquisas envolvendo dados pessoais de crianças e adolescentes, o pesquisador deve refletir sobre a necessidade de protegê-los desde o início, a partir da coleta do material, e planejar todos os tratamentos subsequentes tendo em mente este cuidado especial.

O tratamento de dados pessoais de crianças e adolescentes até 16 (dezesseis) anos incompletos deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal. No caso de adolescentes maiores de 16 (dezesseis) anos, o consentimento pode ser produzido pelo próprio titular dos dados.

Recomenda-se fortemente que as informações sobre o tratamento (e.g. coleta, análise, compartilhamento, eliminação) de dados pessoais de crianças e adolescentes sejam fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento do menor de 16 anos.

Assim que concluída a pesquisa, os dados pessoais poderão ser conservados e seu uso para pesquisas futuras, a princípio, autorizado, devendo o pesquisador justificar sua opção por não anonimizá-los. A conservação deve ser informada no momento de obtenção de consentimento.

Como a base legal para esse tratamento é o consentimento, recomenda-se atenção especial na criação de estrutura para gerir o consentimento e suas revogações, devendo ser consultadas as instâncias competentes do órgão de pesquisa e, eventualmente o Encarregado.

ATENÇÃO! DADOS DE CRIANÇAS E ADOLESCENTES

O tratamento de dados pessoais de **crianças e adolescentes até 16 (dezesseis) anos incompletos** deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

16.2 PESQUISA COM DADOS PESSOAIS DE ACESSO PÚBLICO

Há dois sentidos no uso da expressão “dados públicos”: (i) dados controlados pelo Poder Públicos; e ii) dados cujo acesso é público. Os dados pessoais podem ser públicos em um sentido e não no outro. Por exemplo, no caso de dados disponibilizados em redes sociais (e.g. Twitter), há um agente privado que concede acesso público, a depender da configuração escolhida pelo usuário, configurando dado público no segundo sentido. Por outro lado, podem existir dados pessoais controlado pelo Poder Público cujo acesso não é público (e.g. bases internas de acesso restrito), mas que podem ser compartilhados com órgãos de pesquisa com a finalidade específica de realização de pesquisa. **Nessa seção, será discutido o tratamento de dados pessoais de acesso público.**

No contexto da pesquisa, o uso de dados pessoais cujo acesso é público deve considerar a finalidade, a boa fé e o interesse público que justificaram sua disponibilização. O fato de o dado pessoal ser de acesso público não significa que ele possa ser utilizado como se bem entender, ainda que para a finalidade de realização de pesquisa.

Nos casos de pesquisas que façam uso de dados pessoais de acesso público, é fundamental que haja uma justificativa específica (e.g. justificativa metodológica) para que essas informações não sejam anonimizadas. No caso em que a anonimização não seja possível, recomenda-se a utilização de técnicas de pseudonimização que não prejudiquem a realização do estudo.

Um exemplo interessante são os estudos realizados a partir de informações de ações judiciais nos

websites dos tribunais brasileiros, como o Supremo Tribunal Federal. Nesses estudos, são construídas bases de dados constando informações sobre o nome das partes/proponentes; assistentes simples/terceiros/interessados; resumo; relator; relevância; classificação do STF; datas relevantes; apensos/apensados; pauta; liminar; mérito; *amicus curiae* requerido; *amicus curiae* apreciado; etc. O fato de o dado ser público (disponível para todos no site do STF) não exclui o fato de que o dado é pessoal.

Caso não haja justificativa específica (e.g. metodológica) para exibir os dados pessoais (e.g. nomes de pessoa física, no caso, das partes) de maneira tão clara e direta e a anonimização completa nesse caso é impossível (uma simples consulta no site do STF por meio do número do processo serviria para identificar as partes), a orientação é realizar a pseudonimização, isto é, trocar os nomes das pessoas físicas por um código, dificultando a identificação daqueles por terceiros, se possível.

ATENÇÃO! PESQUISAS COM DADOS DE ACESSO PÚBLICO

Nos casos de pesquisas que façam uso de dados pessoais de acesso público, é fundamental que haja uma **justificativa específica** para que essas informações não sejam anonimizadas. No caso em que a **anonimização** não seja possível, recomenda-se a utilização de técnicas de **pseudonimização** que não prejudiquem a realização do estudo.

16.3 PESQUISA COM DADOS DE SAÚDE

Dados de saúde são considerados dados sensíveis pela LGPD e, portanto, devem ser tratados com maior cuidado. No caso de realização de estudos em saúde pública, órgãos de pesquisa poderão ter acesso à bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas de cada área.

Importante deixar claro que, nesses casos, a divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa, seja em conferências, periódicos científicos etc., em nenhuma hipótese poderá revelar dados pessoais. Não é permitida ainda, em circunstância alguma, a transferência dos dados a terceiros. Por fim, o órgão de pesquisa responsabiliza-se pela segurança dos dados, devendo tomar precauções compatíveis com a sensibilidade dos dados envolvidos.

	**ATENÇÃO! PESQUISA COM DADOS DE SAÚDE** Dados de saúde são considerados **dados sensíveis** pela LGPD e, portanto, devem ser tratados com maior cuidado. Os órgãos de pesquisa poderão ter acesso à bases de dados pessoais, que serão tratados **exclusivamente dentro do órgão** e estritamente para a **finalidade de realização** de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de **segurança** previstas em regulamento específico e que incluam, sempre que possível, a **anonimização ou pseudonimização** dos dados, bem como considerem os devidos padrões **éticos** relacionados a estudos e pesquisas de cada área.

16.4 PESQUISA COM DADOS DE BASES DE DADOS DO PRÓPRIO ÓRGÃO DE PESQUISA (E.G. BASE DE DADOS DE ALUNOS, FUNCIONÁRIOS, PROFESSORES)

Por vezes, pesquisadores ocupam outras posições dentro do órgão de pesquisa (e.g. coordenação de curso, direção de escola etc.), e têm acesso privilegiado a uma série de bases de dados contendo dados pessoais de alunos e colaboradores da instituição.

De toda forma, é importante ressaltar que, regra geral, tais informações foram originalmente obtidas para finalidade diversa da realização de pesquisa. Embora entenda-se que o tratamento subsequente, para realização de estudo por órgão de pesquisa seja permitido pela LGPD, recomenda-se que esse novo uso seja aprovado pelo comitê de ética ou integridade da Instituição de Pesquisa ao qual o projeto esteja vinculado. Ademais, recomenda-se que as informações a respeito desses tratamentos subsequentes sejam comunicadas aos titulares dos dados.

ATENÇÃO! PESQUISA COM DADOS DE SAÚDE

Informações foram originalmente obtidas para determinada pesquisa **não podem ser utilizadas para finalidade diversa**. Qualquer novo uso precisa ser aprovado pelo comitê de ética ou integridade ao qual o projeto esteja vinculado, recomendando-se que as informações a respeito desses tratamentos subsequentes sejam comunicadas aos titulares dos dados.

17. CONSIDERAÇÕES FINAIS

Este Guia destina-se a oferecer algumas diretrizes e boas práticas no tema de Proteção de Dados Pessoais em Pesquisa.

Busca-se apresentar orientações à interpretação da legislação aplicável, ressalvando-se posteriores entendimentos de autoridades competentes ou regulamentações específicas.

Esse documento é suscetível de constante mudança e atualização.

REFERÊNCIAS

BRASIL. **LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS**. Lei nº 13.709, de 14 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 1 ago. 2020.

Commission Nationale de l'Informatique et des Libertés. **Deliberation no. 2017-012 of 19 January 2017 on the adoption of a recommendation relating to passwords.** Disponível em: <https://www.cnil.fr/sites/default/files/atoms/files/recommandation_passwords_en.pdf>. Acesso em: 16 nov. 2020.

DETERMANN, Lothar. **Guia de Campo de Determann sobre o Direito à Privacidade de Dados: Compliance Corporativo Internacional**. 4ª edição. Rio de Janeiro: Lumen Juris, 2019.

EUROPEAN DATA PROTECTION SUPERVISOR. **A Preliminary Opinion on Data Protection and Scientific Research**. Disponível em :<https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf>. Acesso em: 16 nov. 2020.

INFORMATION COMMISSIONER'S OFFICE. **Investigation into the use of data analytics in political campaigns.** A report to Parliament. 6 November 2018. Disponível em: <https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf>. Acesso em: 16 nov. 2020.

INFORMATION COMMISSIONER'S OFFICE. **Guide to the General Data Protection Regulation (GDPR).** Disponível em: < https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/can-we-identify-an-individual-indirectly/>. Acesso em: 16 nov. 2020.

PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA. **GENERAL DATA PROTECTION REGULATION – EU 2016/679.** Disponível em: <https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=pt>. Acesso em: 12 jun. 2020.

FGV DCI

DIRETORIA DE
CONTROLES INTERNOS