Contribuições no Documento Opine - Aqui

Número: OP-616600

Data: 06/02/2024 - 16:40

Resumo: :"teste fabíola","616594":"teste fabiola

Contribuinte: Fabíola de Gabriel Soares Pinto

Número: OP-618137

Data: 08/02/2024 - 09:58

Resumo: "Para com esse processo e elaborar um termo em que somente o Governo Federal, Estadual e Municipal possam fazer consultas ou inspeção que utilizem os dados dos cidadãos. Qualquer entidade fora disso, tem que solicitar formalmente autorização. Nenhum dado deve ser comercializado. ","616594":"Aumentar o espaço para opinião. Fico preocupado que a ANPD esteja focada na anonimização e não esteja atuando na comercialização dos dados dos cidadãos por empresas como SERPRO e DAtAPREV, por exemplo.

Contribuinte: Paulo Cesar Bitar

Número: OP-627551

Data: 22/02/2024 - 09:41

Resumo: :"Acreditamos existir espaço para uma extensão do assunto com preconizando características técnicas de algoritmos, sistemas e certificações das soluções pela ANPD ou INMETRO adequadas às necessidades no âmbito Brasileiro. ","616594":"Somos da Hardprot uma empresa brasileira que tem notória experiência em projetos e no desenvolvimento de soluções brasileiras que envolvem criptografia e pseudonimização, hoje já temos projetos em empresas e agencias de governo, um das mais especializadas no tema no Brasil e Latam.

Contribuinte: FERNANDO AMAURY PEREIRA

Número: OP-627666

Data: 22/02/2024 - 13:35

Resumo: "O estudo apresenta-se condizente com a realidade, felizmente a ANPD decidiu não surfar a onda da anonimização absoluta, já que é uma utopia. O documento apresenta

Ofício n° 09-SG-GT-Ano/2024

Curitiba/PR, 26 de fevereiro de 2024

À Autoridade Nacional de Proteção de Dados (ANPD)

GABINETE DA PRESIDÊNCIA DA REPÚBLICA

Conselho Diretor

Esplanada dos Ministérios, Ministério da Economia, Bloco C, 2º andar, Brasília - DF, 70297-400.

Ao Senhor Waldemar Gonçalves Ortunho Júnior – Diretor Presidente

Atendendo ao Estatuto Social do Instituto Nacional de Proteção de Dados (INPD) e visando apoiar o desenvolvimento do ambiente nacional de proteção de dados pessoais, a observância dos direitos fundamentais de privacidade e proteção de dados, bem como colaborar com o desenvolvimento de políticas públicas relacionadas a proteção de dados pessoais, o INPD vêm, respeitosamente, apresentar suas observações e recomendações quanto à Consulta **Pública** relacionada ao **Estudo Preliminar Anonimização e pseudonimização para a proteção de dados pessoais**, conforme exposto abaixo.

Instituto Nacional de Proteção de Dados - INPD

Atílio Augusto Segantin Braga

(Secretário Geral)

ATILIO AUGUSTO SEGANTIN BRAGA:11825759863

Assinado de forma digital por ATILIO AUGUSTO SEGANTIN BRAGA:11825759863
Dados: 2024.02.26 12:26:57 -03'00'

Contribuição do Instituto Nacional de Proteção de Dados – INPD

Consulta Pública – Estudo Preliminar Anonimização e pseudonimização para a proteção de dados pessoais

Grupo de Trabalho

O presente estudo foi elaborado pelo grupo técnico composto por alguns associados do IINPD e que analisou a sugestão de minuta apresentada pela Autoridade Nacional de Proteção de Dados – ANPD via – "Estudo Preliminar sobre Anonimização e Pseudonimização para a Proteção de Dados Pessoais".

Para garantir uma análise aprofundada e abrangente, contamos com a participação dos seguintes membros do INPD que foram responsáveis pela elaboração do presente estudo:

- Atilio Augusto Segantin Braga
- Denise Nunes
- Martha Leal
- Matheus Passos
- Mitye Hirye
- Rafael Reis

Reconhecimento

Parabenizamos a Autoridade Nacional de Proteção de Dados – ANPD, bem como todos os servidores e colegas que participaram da elaboração do material objeto da presente consulta pública.

Percebe-se um grande esforço no sentido de buscar simplificar a compreensão do processo de Anonimização e Pseudonimização face a sua complexidade e impactos de ordem prática na esfera dos direitos individuais.

Assim, com o objetivo de contribuir e somar a esse esforço, tecemos aqui as contribuições do Instituto Nacional de Proteção de Dados sobre o tema, buscando aperfeiçoar o material, deixando-o mais completo, fluído e de fácil utilização, independente da área de formação de quem o esteja utilizando.

O estudo foi estruturado por tópico seguindo o racional do estudo preliminar.

As sugestões são precedidas da expressão [inclusão] quando o tema ou parágrafo não foi abordado no estudo original. Em se tratando de alterações, é citado o tópico, seção e item, precedido da transcrição do texto original seguindo da sugestão e justificativa de alteração.

Sumário

2. Conceitos Básico

2.1. Glossário

[inclusão]

Minuta atual: Não existe previsão

Sugestão:

Atributo: Também chamado de campo de dados, coluna de dados, ou variável. Uma informação que pode ser encontrada nos registros do conjunto de dados. Nome, gênero e endereço são exemplos de atributos.

Fonte: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation_v1-(250118).pdf

Justificativa: Entendemos ser relevante incluir o conceito de um atributo para fins de clarificação do conceito e para não deixar dúvidas quanto ao seu significado.

Minuta atual:

Banco de dados: Conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

Sugestão:

Banco de Dados: É uma coleção organizada de dados que permite o armazenamento, a recuperação e a manipulação de dados. Geralmente é controlado por um sistema de gerenciamento de banco de dados (DBMS). Pode conter vários conjuntos de dados e tem capacidade para consultar, inserir, atualizar e manipular dados. Um banco de dados também pode ser composto por tabelas, que por sua vez consistem em linhas e colunas. Cada linha representa uma entrada de dados específica e cada coluna representa um atributo ou característica dessa entrada. Os bancos de dados são geralmente usados em aplicações onde os dados precisam ser persistentes e manipulados por várias transações.

Fonte: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation_v1-(250118).pdf

Justificativa: Entendemos que o conceito precisa ser mais abrangente.

Minuta Atual: Não existe previsão

Sugestão:

Classe de equivalência: Os registros em um conjunto de dados que partilham os mesmos valores com certos atributos, tipicamente identificadores indiretos.

Fonte: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation_v1-(250118).pdf

Justificativa: Entendemos ser relevante incluir o conceito de classe de equivalência para fins de clarificação do conceito e para não deixar dúvidas quanto ao seu significado.

Minuta Atual: Vide Banco de Dados.

Sugestão:

Conjunto de Dados: É uma coleção não estruturada ou estruturada de informações que pode estar contida em um arquivo ou em múltiplos arquivos. Pode ser composto por uma variedade de tipos de dados, como texto, números, imagens, vídeos, etc. Um conjunto de dados é usado em análises de dados e geralmente é extraído de um ou mais bancos de dados ou fontes de dados externas. Um conjunto de dados pode ser armazenado por exemplo em formatos como CSV, Excel, JSON, XML, entre outros.

Fonte: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation_v1-(250118).pdf

Justificativa: Na nossa percepção há diferenças entre banco de dados e conjunto de dados, em especial pelo fato de que um conjunto de dados pode não estar necessariamente em um banco de dados no seu conceito literal.

Minuta Atual: Não existe previsão no glossário.

Sugestão:
Conjunto de dados anonimizado: O conjunto de dados resultante após as técnicas de anonimização terem sido aplicadas em combinação com a avaliação de risco adequada.
Fonte: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation_v1-(250118).pdf

Justificativa: Entendemos ser relevante incluir o conceito para fins de clarificação e para não deixar dúvidas quanto ao seu significado.

Minuta Atual: Não existe previsão

Sugestão:
Conjunto de dados original: O conjunto de dados antes de qualquer técnica de anonimização ser aplicada.
Fonte: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation_v1-(250118).pdf

Justificativa: Entendemos ser relevante incluir o conceito para fins de clarificação e para não deixar dúvidas quanto ao seu significado.

Minuta Atual: Não existe previsão

Sugestão:

Identificabilidade vs Re-identificabilidade: O grau ao qual um indivíduo pode ser

identificado em um ou mais conjuntos de dados que contêm identificadores diretos e indiretos, vs o grau ao qual uma pessoa natural pode ser identificada a partir de conjuntos de dados anonimizados.
Fonte: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation_v1-(250118).pdf

Justificativa: Entendemos ser relevante incluir o conceito para fins de clarificação e para não deixar dúvidas quanto ao seu significado.

Minuta Atual: Não existe previsão

Sugestão:

Não identificador: Conjunto de dados que podem conter atributos de dados que não são categorizados como identificadores diretos nem indiretos. Tais atributos não precisam de ser sujeitos a anonimização.
Fonte: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation_v1-(250118).pdf

Justificativa: Entendemos ser relevante incluir o conceito para fins de clarificação e para não deixar dúvidas quanto ao seu significado.

2.2. Anonimização e Pseudonimização de Dados na LGPD

[inclusão]

Minuta atual: Não existe previsão

Sugestão: APÓS O ITEM 22, inclusão do seguinte texto:

A anonimização tem como objetivo a eliminação ou redução significativa dos riscos de reidentificação dos dados anonimizados, mas sempre preservando a veracidade dos resultados do seu tratamento. O processo de anonimização, além de evitar a identificação do titular de dados pessoais, deve garantir que o tratamento realizado após a anonimização não implique em uma distorção dos dados reais.

Em suma, uma análise massiva de dados anonimizados não poderá produzir resultado diferente daquela obtida através de dados não anonimizados.

JUSTIFICATIVA DO ACRÉSCIMO:

A sugestão do acréscimo se dá em razão da necessidade de registrar que o objetivo final do processo de anonimização é a diminuição de riscos de identificação em nível razoável de segurança, evitando-se assim, o estímulo a processos que não possuam técnicas de segurança suficientes para garantir a desvinculação dos dados pessoais às pessoas físicas e a não reversão do processo.

Assegurar que o resultado do tratamento após a anonimização dos dados reflita fielmente o resultado que seria atingido sem a aplicação da anonimização também é de extrema relevância, a medida em que, além de não identificar o titular de dados é preciso reproduzir a realidade da análise de dados que teria sido obtida através dos dados não anonimizados.

https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/guia-y-herramienta-basica-de-anonimizacion

3. OS PROCESSOS DE ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO DE DADOS

3.1. ASPECTOS JURÍDICOS RELEVANTES

3.1.2 RISCOS DE REIDENTIFICAÇÃO DE DADOS ANONIMIZADOS

[inclusão]

Minuta atual: Não existe previsão

Sugestão: APÓS O ITEM 46, inclusão:

É recomendável que se realize uma análise de risco do processo de anonimização por parte do responsável pelo tratamento de dados, através da elaboração de um RIPD.

JUSTIFICATIVA DO ACRÉSCIMO:

A sugestão do acréscimo se dá em razão da constatação de que nenhuma técnica de anonimização poderá garantir em termos absolutos a impossibilidade de reidentificação e que deverá ser mitigada através da gestão de riscos.

https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/guia-y-herramienta-basica-de-anonimizacion

3.2. O PROCESSO DE ANONIMIZAÇÃO

Item 54.

Minuta atual:

Convém ressaltar que os dados que tenham sido tornados irreversivelmente anonimizados deixam de ser considerados "dados pessoais" e o processamento desses dados não exige conformidade com a legislação de proteção de dados. Isso implica que as organizações podem utilizá-los para finalidades, desde que compatíveis, que vão além daquelas para as quais foram originalmente coletados e esses dados podem ser mantidos indefinidamente.

Sugestão:

Convém ressaltar que os dados que tenham sido tornados irreversivelmente anonimizados deixam de ser considerados "dados pessoais" e o processamento desses dados não exige conformidade com a legislação de proteção de dados, desde que, tenham partido de um tratamento lícito e que a finalidade – anonimização - tenha sido informada ao titular.

Justificativa: A redação atual transmite a impressão de que a alegação por parte de um responsável pelo tratamento de dados de possuir um processo anonimização o

liberaria da obrigatoriedade de se adequar a Lei Geral de Proteção de Dados. Apesar do item 29 deixar claro que o processo de anonimização, deve na origem partir de um objeto legítimo de tratamento pelo tratamento, a leitura do item 54 transmite uma impressão equivocada no sentido de que o processo de anonimização isentaria o agente de tratamento quanto a regularidade do tratamento que antecede o processo de anonimização. Por isso, recomendamos que a premissa citada no item 29 fique reforçada logo depois do 54.

Em suma, o Agente de Tratamento de dados necessita possuir um processo lícito de tratamento já que a anonimização se inicia após a coleta, ou seja, é fruto de um processamento de dados que precede de atividades lícitas de tratamento.

Item 55

Minuta atual:

O processo de anonimização, orientado por uma abordagem baseada em riscos, tem como objetivo fornecer um conjunto mínimo de etapas que podem servir de guia de boas práticas aos agentes de tratamentos de dados. Essas etapas sugerem que o agente identifique e compreenda os riscos envolvidos em sua atividade, bem como adote medidas para mitigá-los.

Sugestão

O processo de anonimização, orientado por uma abordagem baseada em riscos, tem como objetivo fornecer um conjunto mínimo de etapas que podem servir de guia de boas práticas aos agentes de tratamentos de dados. Essas etapas sugerem que o **Controlador dos Dados** identifique e compreenda os riscos envolvidos em sua atividade, bem como adote medidas para mitigá-los, **podendo utilizar a metodologia do item 76 ou outra que melhor se adequar ao seu contexto.**

Justificativa do acréscimo

Considerando que o Controlador é responsável pela tomada de decisões referente ao tratamento de dados pessoais, se faz necessário enfatizar a sua responsabilidade no processo de anonimização, visando a minimizar o risco de identificação do titular.

3.2.2. Gestão do risco de reidentificação

[inclusão]

Minuta atual: Não existe previsão

Sugestão: APÓS O ITEM 75, inclusão:

É recomendável que no desenvolvimento de um processo de anonimização seja definida a equipe de trabalho com base em perfis e funções necessárias para o bom desempenho do projeto, bem como o detalhamento do escopo de cada atuação. Alguns perfis que devem ser considerados:

- Responsável pelo tratamento de dados;
- Encarregado de Dados;
- Responsável pelo tratamento de informações anonimizadas;
- Equipe de avaliação de risco;
- Equipe de pré-anonimização e de anonimização;
- Equipe do processo de segurança da informação.

JUSTIFICATIVA DA SUGESTÃO DO ACRÉSCIMO:

A sugestão de acréscimo se dá em função da necessidade de criação de uma equipe para definição do processo de anonimização e agentes envolvidos, garantido a segregação de funções, a confidencialidade e a criação de um inventário para orientação no planejamento do processo de anonimização.

https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/guia-y-herramienta-basica-de-anonimizacion

[inclusão]

APÓS O ITEM 75, inclusão:

Na hipótese de o processo de anonimização compreender dados pessoais sensíveis, art. 5, II da Lei Geral de Proteção de Dados, é recomendável que se constitua uma equipe para avaliar a viabilidade e riscos do processo de anonimização e elaboração de um relatório de viabilidade que conterá de forma detalhada as razões e condições específicas para a anonimização de dados pessoais sensíveis. A equipe responsável pela segurança da informação validará ou não a Análise de Impacto à Proteção de Dados- AIPD, e caso optem por não o fazer, devem emitir um parecer fundamentado.

JUSTIFICATIVA DA SUGESTÃO DE ACRÉSCIMO:

A sugestão de acréscimo se dá em função da análise do potencial de riscos gerados por uma possível reidentificação de dados sensíveis anonimizados e impactos negativos. A comprovação por parte do responsável de tratamento de dados, na adoção de boas práticas e medidas preventivas na fase pré-anonimização se enquadra nos princípios de prestação de contas, segurança e prevenção do art. 6º. da LGPD e art. 40 da mesma norma legal .

[inclusão]

ACRÉSCIMO DE ITEM, com a seguinte redação:

É de extrema relevância o treinamento da equipe envolvida com o processo de anonimização e com dados anonimizados, especialmente no que tange aos requisitos de segurança da informação estabelecidos no art. 46 da LGPD.

O treinamento deverá compreender:

- Princípios e aplicação da política de anonimização;
- Objetivos definidos na gestão de riscos;

- Estrutura e responsabilidade da equipe de trabalho envolvida no processo de anonimização;
- Objetivos e finalidade da informação anonimizada;
- Variáveis de anonimização: identificação e classificação;
- Técnicas de anonimato utilizadas;
- Termos de uso e acesso a informações anonimizadas;
- Medidas de controle para pessoal com acesso a informações anonimizadas;
- Obrigações e deveres em caso de quebra da cadeia de anonimização que acarrete reidentificação dos titulares de dados.

JUSTIFICATIVA DA SUGESTÃO DE ACRÉSCIMO:

A justificativa da sugestão de acréscimo se dá em função da importância da adoção de boas práticas por parte do responsável de tratamento que optar pela anonimização dos dados com a finalidade de prevenção e mitigação de riscos. O treinamento da equipe humana envolvida com o processo é elementar para que se evitem e mitiguem riscos.

https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/guia-y-herramienta-basica-de-anonimizacion

[inclusão]

ACRÉSCIMO DE ITEM, com a seguinte redação:

Tendo em vista que o processo de anonimização não garante de forma absoluta a possibilidade de reidentificação do titular de dados, algumas garantias para preservar os direitos dos interessados são recomendáveis de adoção, por parte do responsável pelo processo de anonimização. São elas:

- Acordos de confidencialidade envolvendo o responsável pelo tratamento, o responsável pelo processo de anonimização, o responsável pelo tratamento de dados anonimizados e pelas pessoas com acesso às informações anonimizadas.
- Termo de Compromisso do destinatário da informação em manter a informação anônima e a obrigação de informar o responsável pelo tratamento em caso de suspeita de reidentificação.
- Realização de auditorias pelo responsável de tratamento ao responsável pelo tratamento de dados anonimizados.

JUSTIFICATIVA DA SUGESTÃO DE ACRÉSCIMO:

A justificativa da sugestão do acréscimo se dá em função de que as garantias adotadas pelo responsável do tratamento, além de configurarem boas práticas com caráter preventivo, serão consideradas em eventual realização de DPIA, como salvaguardas destinadas a minimizar danos em caso de eventual reidentificação de dados pessoais.

Item 81. 9

Minuta atual:

9. Registro e Documentação: mantenha registros detalhados de todas as atividades de pseudonimização, incluindo datas, técnicas utilizadas, responsáveis e propósitos. Isso é importante para fins de prestação de contas, rastreabilidade e registro de operações.

SUGESTÃO

9. Registro e Documentação: mantenha registros detalhados de todas as atividades de pseudonimização, incluindo datas, técnicas utilizadas, responsáveis e propósitos. Isso é importante para fins de prestação de contas, rastreabilidade e registro de operações. **A informação sobre o tipo de pseudonimização poderá ser informado no RIPD, sendo seu preenchimento de responsabilidade do controlador que realizou a pseudonimização .**

Justificativa:

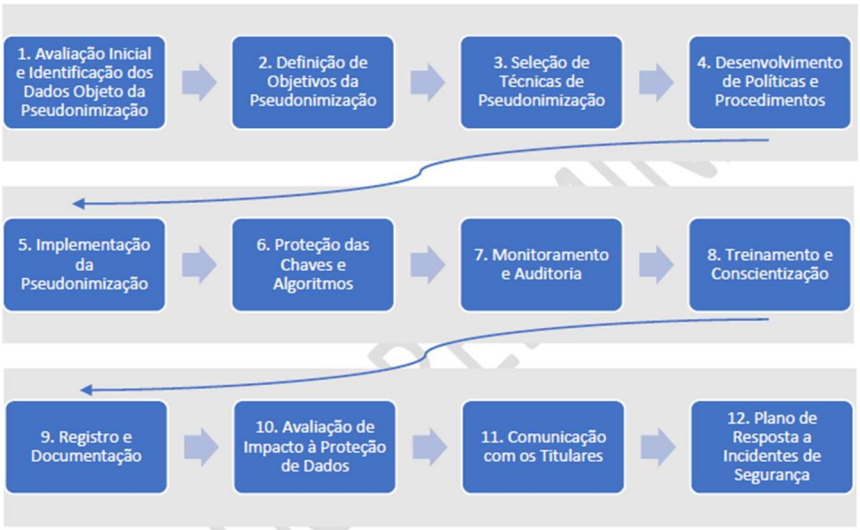
*** Não ficou claro papéis e responsabilidades.

Visto que foi indicado uma métrica para validar o nível de proteção à técnica utilizada (RRA, RRM, quem será o responsável por medir e eficácia da métrica e onde essa informação será utilizada. Ex.: Uma vez feito um RIPD da atividade, essa métrica deverá constar no relatório?

Minuta atual: Item 83

83. Desenvolver uma metodologia eficaz de pseudonimização de dados pessoais, alinhada com as melhores práticas de mercado e em conformidade com os princípios da LGPD é fundamental para garantir a privacidade e a segurança das informações pessoais.

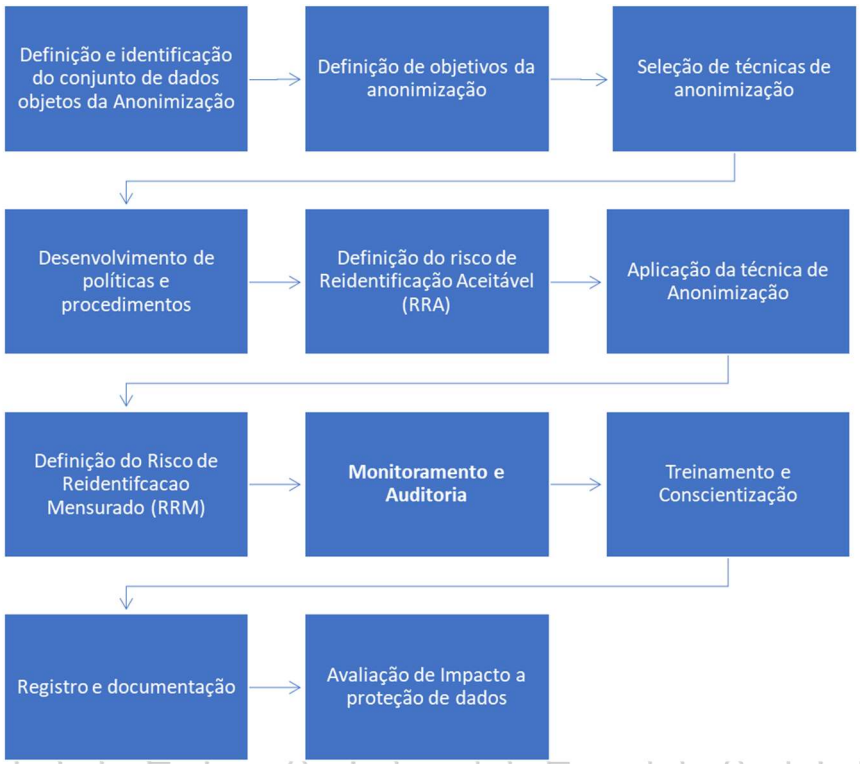
Figura 3: Metodologia Eficaz de Pseudonimização.



Fonte: Elaboração própria.

Sugestão:

Desenvolvimento de uma metodologia eficaz de anonimização de dados pessoais pelo controlador de dados, alinhada com as melhores práticas do mercado e em conformidade com os princípios da LGPD é fundamental para garantir a privacidade e a segurança das informações pessoais:



Justificativa conjunta ao final (item 83 e 84)

Minuta atual: Item 84 – PÁGS. 23-25

84. Conforme ilustração acima (Figura 3), para o desenvolvimento dessa metodologia algumas etapas devem ser observadas:

1. Avaliação Inicial e Identificação dos Dados Objeto da Pseudonimização: inicie com uma avaliação abrangente de quais dados pessoais serão coletados e tratados. Identifique quais dados pessoais serão objeto da pseudonimização, considerando os riscos e o tratamento realizado, dando ênfase a dados considerados sensíveis, como por exemplo, dados de saúde, origem racial ou étnica, convicção religiosa, opinião política, entre outros.

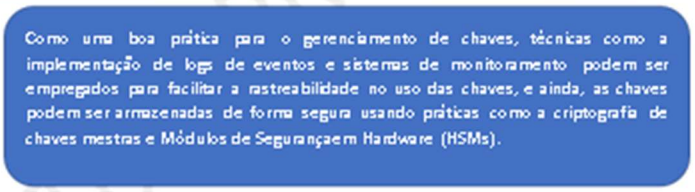
2. Definição de Objetivos da Pseudonimização: estabeleça claramente os objetivos da pseudonimização, incluindo a proteção da privacidade do titular dos dados, a redução do risco de violações de dados e o cumprimento da LGPD.

3. **Seleção de Técnicas de Pseudonimização:** escolha as técnicas de pseudonimização apropriadas com base na natureza dos dados. Isso pode incluir o mascaramento de informações pessoais, o uso de tokenização, o embaralhamento de dados ou a criptografia, dentre outros. A escolha dependerá das características específicas dos dados e dos riscos associados.

4. **Desenvolvimento de Políticas e Procedimentos:** crie políticas e procedimentos claros para garantir a pseudonimização adequada. Isso inclui diretrizes sobre como realizar a pseudonimização, armazenar chaves criptográficas de forma segura e garantir a rastreabilidade e o acesso somente a pessoal autorizado.

5. **Implementação da Pseudonimização:** implemente as técnicas de pseudonimização de acordo com as políticas e procedimentos estabelecidos. Certifique-se de que todos os dados pessoais sejam adequadamente pseudonimizados antes de serem armazenados ou processados. Em alguns casos, técnicas diferentes podem ser aplicadas, concomitantemente, para produzir uma pseudonimização eficiente.

6. **Proteção das Chaves e Algoritmos:** garanta que as chaves e algoritmos utilizados no processo de pseudonimização, como por exemplo, chaves criptográficas, senhas de acesso a sistemas ou a arquivos, códigos-fonte, dentre outros, sejam armazenadas de forma segura e acessíveis apenas a pessoal autorizado. Os registros de auditoria devem ser mantidos, documentando quando as chaves foram usadas, quem as utilizou e com que finalidade. Isso é valioso para conformidade regulatória, registro de operações e investigações de segurança. É fundamental garantir que os dados possam ser revertidos quando necessário de forma segura, pelo controlador.



7. **Monitoramento e Auditoria:** implemente sistemas de monitoramento e auditoria para verificar continuamente a eficácia da pseudonimização e garantir o cumprimento das políticas e procedimentos. Realize revisões e auditorias regulares a fim de acompanhar as mudanças regulatórias, tecnológicas e melhores práticas de mercado relacionadas à pseudonimização e ajuste sua metodologia conforme necessário.

8. **Treinamento e Conscientização:** forneça treinamento regular aos colaboradores que lidam com dados pessoais para garantir que compreendam a importância da pseudonimização e saibam como aplicá-la corretamente.

9. **Registro e Documentação:** mantenha registros detalhados de todas as atividades de pseudonimização, incluindo datas, técnicas utilizadas, responsáveis e propósitos. Isso é importante para fins de prestação de contas, rastreabilidade e registro de operações.

10. **Relatório de Impacto à Proteção de Dados:** realize a avaliação de impacto sobre a proteção de dados, elaborando o Relatório de Impacto

à Proteção de Dados Pessoais (RIPD) quando apropriado, a fim de avaliar os riscos associados à pseudonimização e garantir a conformidade com a LGPD.

11. Comunicação com os Titulares: esteja preparado para informar de forma transparente e acessível aos titulares sobre a pseudonimização e os direitos de acesso e correção de suas informações pessoais, conforme exigido pela LGPD.

12. Plano de resposta a Incidentes de Segurança: desenvolva um plano de resposta a incidentes de segurança com dados pessoais que inclua procedimentos para lidar, entre outras situações, com acessos não autorizados e tratamentos inadequados ou ilícitos, incluindo as ações de mitigação apropriadas para reverter ou mitigar os efeitos dos prejuízos gerados.

Sugestão:

84. Conforme ilustração acima, para o desenvolvimento dessa metodologia algumas etapas devem ser observadas:

1. **Definição e identificação do banco de dados objetos da Anonimização:** Inicie com a definição e identificação do conjunto de dados que serão objeto de anonimização, considerando os riscos, tratamento realizado e finalidade.

2. **Definição de Objetivos da Anonimização** : estabeleça claramente os objetivos da Anonimização , incluindo a proteção da privacidade do titular dos dados, a redução do risco de violações de dados e o cumprimento da LGPD.

3. **Seleção de técnicas de anonimização**: escolha as técnicas de anonimização apropriadas com base na natureza dos dados. A escolha dependerá das características específicas dos dados e dos riscos associados.

4. **Desenvolvimento de Políticas e Procedimentos**: crie políticas e procedimentos claros para garantir a anonimização adequada.

5. **Definição do risco de Reidentificação Aceitável (RRA):** definir o risco de reidentificação aceitável (RRA), para um certo conjunto de dados, considerando o contexto do agente de tratamento.

6. **Aplicação da técnica de anonimização:** implemente as técnicas de anonimização de acordo com as políticas e procedimentos estabelecidos. Certifique-se de que todos os dados pessoais sejam adequadamente anonimizados antes de serem armazenados ou processados.

7. Definição do Risco de Reidentifcacao Mensurado (RRM): definir o risco de reidentificação aceitável (RRA), para um certo conjunto de dados, considerando o contexto do agente de tratamento.

8. Monitoramento e Auditoria: implemente sistemas de monitoramento e auditoria para verificar continuamente a eficácia da anonimização e garantir o cumprimento das políticas e procedimentos. Realize revisões e auditorias regulares a fim de acompanhar as mudanças regulatórias, tecnológicas e melhores práticas de mercado relacionadas à anonimização e ajuste sua metodologia conforme necessário.

9. Treinamento e Conscientização: forneça treinamento regular aos colaboradores que lidam com dados pessoais para garantir que compreendam a importância da anonimização e saibam como aplicá-la corretamente.

10. Registro e documentação: mantenha registros detalhados de todas as atividades de anonimização, incluindo datas, técnicas utilizadas, responsáveis e propósitos. Isso é importante para fins de prestação de contas, rastreabilidade e registro de operações**.**

11. Avaliação de Impacto a proteção de dados : realize a avaliação de impacto sobre a proteção de dados, elaborando o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) quando apropriado, a fim de avaliar os riscos associados à anonimização e garantir a conformidade com a LGPD. Considere a elaboração do RIPD sempre que o tratamento envolve alto risco.

Justificativa da inclusão

A sugestão do acréscimo se dá em virtude da identificação da necessidade de uma metodologia para as etapas do desenvolvimento das atividades no processo da animização, contribuindo para a conformidade com a legislação, mitigação de gaps e prestação de contas para demonstração de aplicação da eficácia das medidas adotadas.

A redação atual não deixa claro papéis e responsabilidades, visto que indica uma métrica para validar o nível de proteção à técnica utilizada (RRA, RRM, quem será o responsável por medir a eficácia da métrica e onde essa informação será utilizada. Ex. Uma vez feito, um RIPD da atividade, essa métrica deverá constar no relatório? Abordaremos o tema com mais profundidade em item específico (item 9).

3.3. O PROCESSO DE PSEUDONIMIZAÇÃO

6. APÊNDICES

APENDICE I. PRINCIPAIS ESCLARECIMENTOS

Minuta atual:

i) A anonimização, geralmente, não reduz a probabilidade de reidentificação de um conjunto de dados a zero - a anonimização não impossibilita a reidentificação de um conjunto de dados; o processo de anonimização e a forma como é implementado terão influência direta na probabilidade de riscos de reidentificação.

SUGESTÃO

i) A anonimização, **geralmente, reduz** a probabilidade de reidentificação de um conjunto de dados de forma significativa - a anonimização **se aplicada com meios apropriados** impossibilita a reidentificação de um conjunto de dados; o processo de anonimização e a forma como é implementado terão influência direta na probabilidade de riscos de reidentificação.

Justificativa

Segundo LGPD no seu art. 5º Para os fins desta Lei, considera-se:

XI - 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;

Porém aqui, leva o leitor a concluir de forma equivocada que não existe anonimização real, uma vez que diz que a anonimização não impossibilita a reidentificação de um conjunto de dados.

Especialmente considerando-se a própria definição de anonimização da 29100: "processo pelo qual dados pessoais são irreversivelmente alterados, de forma que um titular de dados pessoais não mais pode ser identificado, direta ou indiretamente, seja por um controlador apenas ou em colaboração com qualquer outra parte".

*** Falta esclarecer melhor esta definição.

Ref.: ABNT NBR ISO/IEC 29100:2020

4.4.4 Dados pseudonimizados

Os processos de anonimização.... mas destroem a capacidade de vinculação.

APENDICE II. CADERNO DE TÉCNICAS PARA ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO

TÉCNICAS PARA ANONIMIZAR DADOS TEXTUAIS ESTRUTURADOS (PAG. 30)

Minuta atual: (Pág. 30)

Para as colunas Idade e Quantidade filhos o valor do ruído foi trucando

SUGESTÃO

Para as colunas Idade e Quantidade filhos o valor do ruído foi trucando => Confirmar o sentido da palavra "trucando" ou corrigir se for erro de digitação.

TÉCNICAS PARA ANONIMIZAR IMAGENS (PAG. 34/35)

SUGESTÃO DE EXCLUSÃO DO EXEMPLO DE TÉCNICA DE ANONIMIZAÇÃO IMAGENS:

As Técnicas de Desfoque Gaustiano (blur) e pixelização descritas no Guia da ANPD, como ilustrações de técnicas válidas de anonimização, não podem ser admitidas, uma vez que vão de encontro com o disposto na norma legal, especialmente em seu art. 12º.

JUSTIFICATIVA DA SUGESTÃO DE EXCLUSÃO:

A sugestão de exclusão de recomendação das técnicas de anonimização de imagens trazidas no estudo preliminar da ANPD se dá em função de que contraria o disposto na LGPD, especificamente na conceituação do dado anonimizado e do grau de razoabilidade de um processo de anonimização, dispostos nos artigos 5º., III e art. 12º., Caput e Parágrafo Primeiro, senão vejamos:

> "Art. 5, III- Dado anonimizado: dado relativo a um titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião do seu tratamento."
>
> "Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.
>
> &1º. A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios...."

Observe-se que as imagens disponibilizadas no estudo preliminar da ANPD ,como dados anonimizados, não podem assim ser entendidas, uma vez que do singelo olhar da figura já é possível identificar o indivíduo, especialmente se aqueles que a veem já o conhecem. E não se diga, nem por mera hipótese, que o processo de reidentificação do dado anonimizado, não possa se dar através de um terceiro que já tenha tido algum contato visual prévio com o titular de dados que sofreu a técnica de anonimização, objeto de contestação. Pois, a própria norma legal define o dado anonimizado como sendo aquele que não identifica o seu titular.

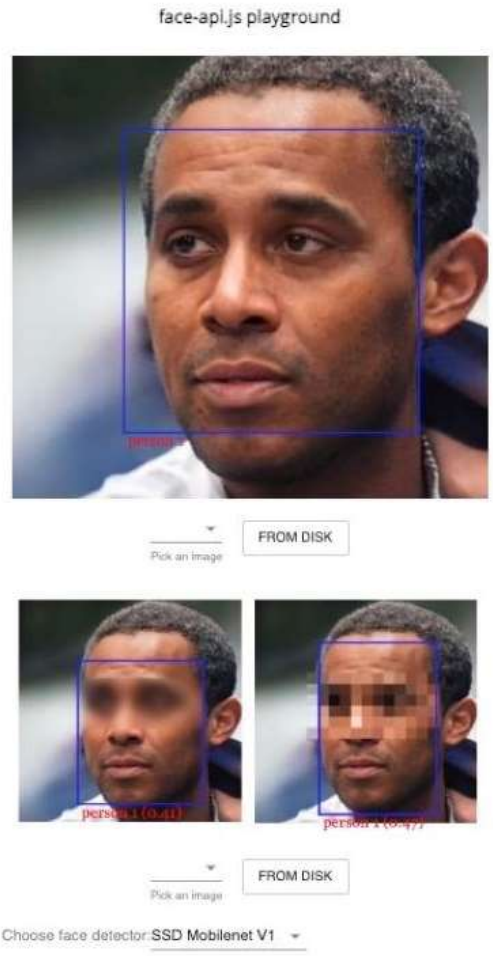
Apenas, por mero exercício, no improvável contexto de acatarmos as figuras da página 35 do Guia como sendo dados anonimizados, precisaríamos enfrentar o disposto no art. 12, Caput e Parágrafo Primeiro.

A lei condiciona o processo de anonimização a dois critérios: i) quando forem utilizados esforços razoáveis para a anonimização; ii) e que esses esforços razoáveis para a reversão do processo levem em conta tempo, custo e tecnologias disponíveis.

Pois bem, partindo da premissa de que o processo de anonimização requer técnicas seguras e que contenham um grau considerável de confiabilidade de não reversão da anonimização, demonstramos a singeleza do processo que levou a reidentificação da imagem em questão.

O aplicativo "face.api.js playground" disponibilizado na internet e de forma gratuita, permite que ao se inserir a imagem das fls. 35 se reverta a imagem a sua forma original, identificando o titular de dados.

Portanto, impõe-se por medida de segurança e evitando a indução de técnicas e processos de anonimização que não sejam seguros, seja suprimido os exemplos de imagens anonimizadas apresentados equivocadamente no Guia.



APENDICE IV. ESTUDO DE CASOS

Caso 03: Compartilhamento de dados educacionais – Supressão, generalização, mascaramento, adição de ruídos e permutação.

Esclarecimentos:

Quando, em quais situações, devemos aplicar a métrica RRA/RRM?

Risco de Reidentificação mensurado (RRM)

Item 7. (Acompanhamento do RRM/RRA) - pág. 48

1) Como acompanhar?
2) Se o compartilhamento envio dos dados for feito uma única vez?
3) Se o compartilhamento for periódico, deve-se toda vez recalcular o RRM? É isso? Não ficou claro.

Minuta atual:

07. De acordo com o processo proposto, é necessário acompanhar o risco mensurado de reidentificação para que ele sempre se mantenha abaixo do risco de reidentificação aceitável.

SUGESTÃO

07. De acordo com o processo proposto, é necessário acompanhar o risco mensurado de reidentificação para que ele sempre se mantenha abaixo do risco de reidentificação aceitável. **Neste caso é responsabilidade do órgão que coleta os dados realizar periodicamente o cálculo do RRM para verificar sua efetividade**.

Justificativa:

Não está claro como deve ser executado.

***

MANIFESTAÇÃO OI – Estudo Preliminar Anonimização e Psedonimização para a proteção de dados pessoais

1. ANONIMIZAÇÃO

1.1. Exigência de compatibilização entre a utilização de dados anonimizados e a finalidade original da coleta

Como é cediço, a LGPD estabelece em seu art. 12 que os dados anonimizados não são considerados dados pessoais para fins de aplicação da LGPD – exceto se o processo puder ser revertido, considerando exclusivamente meios próprios ou esforços razoáveis.

Acertadamente, o guia proposto pela ANPD esclarece que a anonimização é um processo e, como tal, implica em operação de tratamento de dados pessoais, para a qual devem ser aplicados os princípios e regras previstos na LGPD:

> *30. Tal afirmação possui desdobramentos relevantes. Primeiramente, fica evidenciado que o ato inicial do processo de anonimização configura operação de tratamento de dado pessoal, atraindo, assim, a aplicação de princípios e regras da LGPD. O segundo desdobramento é o de que a anonimização não é capaz de per se legitimar atividade de tratamento originalmente ilícita por falta de hipótese legal que lhe dê fundamento.*

Ainda, não há dúvidas de que a **atividade de anonimização** – em sendo a finalidade primordial da coleta – deva ser devidamente informada aos titulares de dados e, em se tratando de um tratamento posterior, deva ser, no mínimo, compatível com a finalidade que justifica o tratamento inicial, também como proposto pelo guia.

Ocorre que, mais adiante, estabelece o parágrafo 54:

> *54. Convém ressaltar que os dados que tenham sido tornados irreversivelmente anonimizados deixam de ser considerados "dados pessoais" e o processamento desses dados não exige conformidade com a legislação de proteção de dados.* ***Isso implica que as organizações podem utilizá-los para finalidades, desde que compatíveis, que vão além daquelas para as quais foram originalmente coletados e esses dados podem ser mantidos indefinidamente***

Apesar de absolutamente correta a primeira parte do parágrafo, entende-se que houve equívoco da autoridade ao condicionar a utilização de dados anonimizados a finalidades compatíveis com a origem da coleta.

Considerando premissa de que dados anonimizados deixam de ser dados pessoais – e por isso mesmo escapam da aplicação da LGPD, a conclusão lógica é de que dados já anonimizados possam ser utilizados livremente pelas organizações, independentemente de qualquer compatibilidade com os fundamentos da coleta.

Novamente, não se nega que a finalidade que justifica o *processo de anonimização* deva ser compatível com a finalidade original, já que o *processo de anonimização* implica em tratamento de dados. Todavia, uma vez anonimizados, os dados deixam de ser pessoais, não havendo necessidade de observância dos princípios e regras de proteção de dados,

como o da necessidade e adequação. Entendimento contrário importaria em aplicação, ainda que indireta da LGPD, o que contraria o disposto no art. 12.

Assim, entendemos que o item deva ser ajustado conforme a seguir:

> *54. Convém ressaltar que os dados que tenham sido tornados irreversivelmente anonimizados deixam de ser considerados "dados pessoais" e o processamento desses dados não exige conformidade com a legislação de proteção de dados.* ***Isso implica que as organizações podem utilizá-los para finalidades, ~~desde que compatíveis,~~ que vão além daquelas para as quais foram originalmente coletados e esses dados podem ser mantidos indefinidamente.***

1.2. Da gestão do risco de reidentificação

Considerando a possibilidade de reidentificação de titulares decorrentes do processo de anonimização, o guia propõe uma metodologia para gestão de riscos consistente em 04 etapas. Trata-se de uma abordagem alinhada à metodologia *risk-based approach*, que considera diversos cálculos matemáticos para determinar o risco de reidentificação.

Apesar de louvável a iniciativa, o processo sugerido pela autoridade é de difícil compreensão e pouco exequível. É preciso destacar que a exigência de cálculos matemáticos complexos nem sempre se mostra a decisão mais acertada a depender do contexto.

Não há dúvidas de que os agentes de tratamento precisam ter condições de demonstrar que as técnicas de anonimização aplicadas consideram os meios próprios e esforços razoáveis disponíveis à época, mas a exigência de um processo como o proposto pode implicar no dispêndio de recursos, como contratação de consultorias para elaboração dos cálculos, dificultando – senão inviabilizando - a adoção de uma medida que, em última instância, tende a beneficiar os titulares de dados.

Entendemos que o guia seja uma importante ferramenta para orientar as organizações sobre as melhores práticas, todavia, não podemos nos esquecer que, se de um lado, cabe à autoridade estabelecer as balizas legais, do outro, cabe aos agentes de tratamento garantir os mecanismos de governança conforme suas diretrizes internas, em razão do princípio de prestação de contas.

Dessa maneira, caso a ANPD queira auxiliar os agentes de tratamento na condução do tema, deve **sugerir** a adoção de modelos mais exequíveis, a exemplo das autoridades europeias, tais como a ICO, que, em seu guia de anonimização[1], dispõe sobre os critérios que devem ser considerados pelas organizações sem definir uma metodologia de avaliação de risco específica, recomendando, em seu lugar, a elaboração de avaliações de impacto conforme orientações já existentes.

Nesse sentido, entendemos que a autoridade poderia apresentar uma alternativa ao modelo de prestação de contas, se valendo, por exemplo, do método *procedure-based approach*, através da qual os agentes de tratamentos documentam os procedimentos adequados para anonimização com base nos riscos detectados previamente. Vale ressaltar que a definição de tais riscos pode ser feita com base em metodologias já praticadas pelas empresas em contextos como relatórios de impacto à proteção de dados ou testes de

[1] https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf

legítimo interesse, considerando os critérios objetivos (custo x tempo) e subjetivos (meios próprios) estabelecidos pela lei.

Ainda que a ANPD entenda relevante a recomendação da metodologia sugerida, entendemos que o guia deva, ao menos, ser revisto para melhor esclarecer como as organizações devem proceder em cada uma das etapas, incluindo o maior número possível de exemplos práticos para subsidiar os agentes de tratamento.

1.3. Conceito de "meios próprios"

O parágrafo 52 do guia dispõe que:

> 52. Diferentemente da noção de "esforços razoáveis", o conceito de meios próprios tem conteúdo mais delimitado, podendo-se afirmar que são meios próprios as habilidades, os dados, instrumentos e técnicas disponíveis ao próprio agente de tratamento responsável pela anonimização. Sendo assim, importa ressaltar que, a partir do texto normativo do art. 12, caput, da LGPD, compreende-se que a avaliação da possibilidade de reidentificação de dados e a reversão do processo de anonimização devem ter em consideração não apenas o uso de meios próprios do agente de tratamento responsável pela anonimização, ***mas também a atuação de outras pessoas ou entidades que, com meios e esforços razoáveis, podem reidentificar conjunto de dados anonimizados.***

Da leitura acima, pode-se interpretar que a noção de "meios próprios" poderia abranger qualquer outra pessoa ou entidade que, com meios e esforços razoáveis, poderiam reidentificar o conjunto de dados anonimizados.

É preciso considerar, no entanto, que a expressão "meios próprios" trata-se de um critério subjetivo, diferentemente da noção de esforços razoáveis, que considera fatores objetivos como tempo, custo e tecnologia disponível. Em sendo subjetiva, tal avaliação não pretende abranger os meios disponíveis no mercado, senão os meios do próprio agente de tratamento, por isso, inclusive, o art. 12 utiliza o adverbio "exclusivamente".

Em verdade, a lei buscou preservar uma análise contextual que permite verificar se, na conjuntura/ambiente de determinada organização, o processo de anonimização poderia ser facilmente revertido, como por exemplo, se o controlador ou operador responsável pela anonimização dispõe de ferramentas internas (hardware ou softwares) ou outro conjunto de dados auxiliares que podem reverter o processo de anonimização sem dificuldades.

A noção de meios próprios, portanto, não deve abranger toda e qualquer organização, mas apenas aqueles agentes que, direta ou indiretamente, possam se valer da base de dados anonimizada.

Nesse sentido, entendemos que o parágrafo possa ser melhor redigido, deixando clara a limitação acima:

> 52. [...] Sendo assim, importa ressaltar que, a partir do texto normativo do art. 12, caput, da LGPD, compreende-se que a avaliação da possibilidade de reidentificação de dados e a

reversão do processo de anonimização devem ter em consideração não apenas o uso de meios próprios do agente de tratamento responsável pela anonimização, ***mas também a atuação de outras pessoas ou entidades que possam se valer dos dados anonimizados e que, com meios e esforços razoáveis, podem reidentificar conjunto de dados anonimizados.***

1.4. Proibição de anonimização inteiramente automatizada

Dispõe o item "K" do Apêndice I: "*A **anonimização não deve ser totalmente automatizada** - ferramentas automatizadas podem ser usadas durante o processo de anonimização, no entanto, dada a importância do contexto e a avaliação geral do processo, poderá ser necessária a intervenção de um especialista humano"*

É certo que o envolvimento humano em processos de anonimização pode ser uma medida a ser recomendada para as organizações, todavia, inexiste na LGPD qualquer proibição de que o processo de anonimização seja automatizado.

Não devemos nos esquecer que os guias produzidos pela ANPD, embora sejam de extrema valia para a correta interpretação da lei, constituem ato infra legal, não podendo inovar ou contrariar a lei em razão do princípio da reserva legal.

Senão por isso, com o desenvolvimento tecnológico, podem surgir ferramentas que realizam a anonimização automatizada, o que deve ser visto como algo positivo, já que permitiria a economia de tempo e recursos pelas empresas.

A limitação acima, portanto, é desarrazoada e contraria o fundamento da LGPD de desenvolvimento tecnológico, além de estabelecer uma proibição sem qualquer respaldo legal. Por esse motivo, entendemos que o item deva ser excluído do apêndice, ou, quando muito, reescrito para deixar claro que se trata de uma simples **recomendação**, e não de uma vedação.

2. PSEUDONIMIZAÇÃO

2.1. Da metodologia de Pseudonimização

Ao abordar sobre os requisitos para uma pseudonimiziação adequada, o guia da ANPD estabelece alguns passos a serem seguidos pelas organizações, incluindo a elaboração de políticas, proteção de chaves, realização de auditorias etc.

Dentre as medidas recomendadas, constam:

> 10. Avaliação de Impacto à Proteção de Dados: realize a avaliação de impacto sobre a proteção de dados, elaborando o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) quando apropriado, a fim de avaliar os riscos associados à pseudonimização e garantir a conformidade com a LGPD. Considere a elaboração do RIPD sempre que o tratamento envolver alto risco.
>
> 11. Comunicação com os Titulares: esteja preparado para informar de forma transparente e acessível aos titulares sobre a

pseudonimização e os direitos de acesso e correção de suas informações pessoais, conforme exigido pela LGPD.

12. Plano de resposta a Incidentes de Segurança: desenvolva um plano de resposta a incidentes de segurança com dados pessoais que inclua procedimentos para lidar, entre outras situações, com acessos não autorizados e tratamentos inadequados ou ilícitos, incluindo as ações de mitigação apropriadas para reverter ou mitigar os efeitos dos prejuízos gerados

As medidas acima destacadas tratam-se, na verdade, de ações inerentes ao programa de governança dos agentes de tratamento, não tendo relação direta com o tema pseudonimização.

A elaboração de um Relatório de Impacto à Proteção de Dados, por exemplo, é deflagrada conforme a atividade de tratamento que justifica a utilização do dado pessoal, não em razão do processo de pseudonimização. Vale ressaltar que a pseudonimização é, sobretudo, uma medida de segurança cujo objetivo é dificultar a identificação do titular, não se tratando de um fim em si mesmo.

Diferentemente do conceito de anonimização, portanto, que exige uma avaliação de risco para considerar a probabilidade de reidentificação do titular, não há que se falar em risco de pseudonimização, já que a atividade de tratamento anterior ao processo de pseudonimização é o que deve deflagrar ou não a avaliação de impacto.

Da mesma forma, a exigência de um plano de resposta a incidentes de segurança ou um canal para exercício de direitos dos titulares são responsabilidades inerentes de qualquer agente de tratamento, independentemente se são tratados dados pseudonimizados ou não.

Especificamente em relação à comunicação com os titulares, salvo melhor juízo, não identificamos qual seria a utilidade de comunicá-los sobre os processos de pseudonimização da empresa. Entendemos que, como medida de segurança, tal informação deva constar em avisos de privacidade, todavia, não há necessidade de acionamento do titular para informar que, em determinada atividade, a empresa procedeu com a pseudonimização dos dados, até porque essa não é a conduta adotada para outras medidas de segurança.

Nesse contexto, entendemos que os itens 10, 11 e 12 devam ser excluídos por não haver relação direta com a atividade de pseudonimização.

28 de fevereiro de 2024

Christian Lopes Kratochwil

Encarregado de Proteção de Dados da Oi

Bruna Fróes de Oliveira

Especialista em Privacidade na Oi

Daiane Conde da Costa

Analista III em Privacidade na Oi

Consulta pública realizada pela Autoridade Nacional de Proteção de Dados (ANPD) - Estudo Preliminar sobre anonimização e pseudonimização para proteção de dados

Setor: ANPD - Coordenação-Geral de Normatização

Abertura: 30/01/2024

Encerramento: 14/03/2024

Contribuições da Confederação Nacional do Comércio de Bens, Serviços e Turismo – CNC

1. Considerando o conteúdo do Estudo Preliminar, apresente suas contribuições sobre o texto.

Itens 29, 30 e 31 do Estudo: O dado anonimizado deixa de ser dado pessoal e dispensa conformidade com a LGPD. Se o tratamento anterior possuía alguma irregularidade, após a anonimização, os dados anonimizados não precisarão ser eliminados, pois não haverá mais tratamento de dados pessoais.

(Contribuição enviada pela Plataforma Participa Mais Brasil.)

2. Gostaria de deixar algum comentário ou sugestão adicional?

Item 34 do Estudo: A anonimização não é uma finalidade que legitima o tratamento de dados pessoais, e sim uma medida de segurança e gestão de riscos. Na fase inicial de coleta de dados, o controlador não tem o dever de informar uma futura e eventual anonimização como uma das finalidades do tratamento.

(Contribuição enviada pela Plataforma Participa Mais Brasil.)

ANEXO

Passamos a destacar os principais **pontos de atenção** do Estudo Preliminar.

- **A anonimização não deve ser considerada uma operação de tratamento de dados pessoais autônoma.**

A consideração da anonimização como atividade de tratamento representaria um equívoco conceitual, em desacordo com o pretendido pelo legislador ao editar a

LGPD. Isso porque, por mais que o rol de atividades previstas como tratamento de dados seja somente exemplificativo, é de se notar que o legislador opta por listar 20 condutas que representem atividades de tratamento (art. 5º, X) para, em seguida, definir o conceito de anonimização (art. 5º, XI). Além disso, seria necessário um input de dado pessoal para, após a anonimização, perder sua associação direta com uma pessoa física.

Dessa maneira, entende-se que a anonimização deveria ser considerada como uma medida técnica acessória destinada a garantir a adequação de uma base de dados à LGPD, seja através da minimização de dados ou da garantia da segurança de uma base de dados.

- **Base legal específica para a atividade de anonimização e princípios da legalidade, adequação e necessidade (LGPD, art. 6º caput, incs. II e III).**

A sugestão de que a anonimização deve se vincular ao princípio da legalidade parte do pressuposto de que o agente de tratamento deverá atribuir uma base legal específica para realizar a anonimização. Entretanto, a anonimização não é um fim em si mesmo, mas uma medida técnica acessória, baseada em riscos, que envolve a aplicação de técnicas e salvaguardas específicas para evitar a reidentificação dos dados. Por esse motivo, entende-se que a base legal atribuída à operação originária deverá ser aproveitada para a realização da anonimização e, ainda, que a anonimização considere as técnicas mais adequadas e os níveis apropriados para o conjunto de dados em questão.

Ao mencionar o princípio da adequação, a Autoridade pretende que a anonimização seja adequada ao tratamento anteriormente realizado. Contudo, a realização da anonimização pressupõe que o conjunto de dados anteriormente tratado perderá o caráter de dado pessoal, não havendo como verificar se o tratamento posterior é ou não adequado às finalidades informadas ao titular. Ademais, realizada a anonimização, sequer é possível falar em tratamento de dados.

Ainda, a vinculação da anonimização ao princípio da necessidade não representa equívoco, mas a linguagem adotada pela ANPD parece sugerir que a anonimização é parte essencial do ciclo de vida do dado. Tal processo não deve ser entendido como etapa obrigatória do tratamento ou como um fim em si mesmo. A anonimização, apesar de ser definida como um dos direitos dos titulares (art. 18, IV), deve ser entendida como uma opção técnica para o encerramento do tratamento de dados por um agente e enquanto uma faculdade do agente, caberá a este demonstrar a necessidade e adequação da aplicação desta medida ao caso concreto.

- **Transparência com o titular sobre as medidas de anonimização e pseudonimização adotadas.**

O Estudo Preliminar fala sobre tornar obrigatória a comunicação ao titular sobre a possível aplicação futura da técnica de anonimização. Porém, isso se se revelaria uma exigência de difícil cumprimento, pois, independentemente da técnica empregada, a anonimização inevitavelmente reduz as informações atreladas aos dados pessoais em questão. Dessa forma, é possível que o controlador não consiga determinar durante o tratamento se a finalidade específica estabelecida no momento da coleta pode ser alcançada de forma adequada com os dados anonimizados. A redação atual sugere um dever de comunicação sobre uma medida técnica que poderia comprometer a utilidade do conjunto de dados para sua finalidade original, o que se mostra como uma obrigação, por vezes, impraticável.

- **Ponderação do binômio anonimização x utilidade como fator orientador acerca do uso da técnica da anonimização a um banco de dados e o grau de vinculação decorrente para os agentes de tratamento.**

O estabelecimento do binômio Utilidade x Anonimização como norte para os agentes de tratamento, ainda que constitua uma relevante orientação, deve ser entendido como uma sugestão.

A anonimização não é a única forma de encerramento do tratamento de dados, sendo uma opção do agente de tratamento e não uma etapa essencial do ciclo de vida do dado. Ou seja, é importante que a ANPD destaque que a anonimização não é um fim em si mesmo ou etapa obrigatória, mas uma medida técnica opcional para o encerramento do tratamento e a minimização de dados.

- **Proposta de metodologia de gestão contínua de risco com grandezas numéricas.**

É bem-vindo o fornecimento de orientações para a gestão do risco em operações de anonimização de dados, estipulando um caráter contínuo para a gestão de riscos que evidencia que a anonimização não é um processo estático e livre de falhas. Sendo assim, o fornecimento de uma metodologia para acompanhamento de riscos é medida que objetiva ajudar os agentes de tratamento a realizar a gestão de suas bases de dados.

Entretanto, o fornecimento de metodologia específica e detalhada pode acabar por sobrecarregar as equipes técnicas responsáveis pela anonimização, motivo pelo

qual destacamos a necessidade de reavaliação do Estudo Preliminar à luz da regulação de agentes de tratamento de pequeno porte.

Além disso, sugerimos a substituição dos critérios numéricos por técnicas de ponderação e análise de proporcionalidade, já comumente utilizadas pelos agentes de tratamento na realização de RIPDs.

- **Comentários sobre técnicas de anonimização e o grau de vinculatividade que tal listagem deve ter para os agentes de tratamento.**

A listagem de técnicas de anonimização e pseudonimização, bem como de suas limitações e potencialidades, deve ser considerada como uma enumeração de exemplos, a fim de facilitar a atividade dos agentes de tratamento.

Desde que efetivamente documentada, a aplicação bem-sucedida de outras técnicas, que não as mencionadas no Estudo Preliminar, devem ser avaliadas em pé de igualdade pelo regulador.

Ademais, a definição das limitações de cada técnica deve ser abordada somente como uma análise não taxativa, devendo cada agente ser capaz de ponderar as potencialidades e aplicações de cada técnica de anonimização adotada durante o processo de gestão do risco.

São Paulo, 28 de fevereiro de 2024.

À
Autoridade Nacional de Proteção de Dados - ANPD
Setor Comercial Norte - SCN, Quadra 6, Conjunto "A", Edifício Venâncio 3000, Bloco "A", 9º andar
CEP 70.716-900 - Brasília – DF

Ref.: Consulta à sociedade de estudo preliminar sobre anonimização e pseudononimização para a proteção de dados pessoais

A/C ANPD - Coordenação-Geral de Normatização

Exmos Srs. e Sras.,

1. A **Associação Brasileira das Empresas de Cartões de Crédito e Serviços – Abecs** e a **Federação Brasileira de Bancos (FEBRABAN)**, entidades representativa dos setores de meios de pagamento e bancário brasileiros, vêm apresentar suas contribuições à Consulta Pública em referência, as quais se encontram anexas a este documento, na forma de comentários, destacados em amarelo, item a item, do Estudo Preliminar.

2. Esperamos que nossos apontamentos, sejam considerados e possam auxiliar qualitativamente o Estudo Preliminar realizado por esta Autoridade.

Ficamos à disposição para esclarecimentos que V.S.as julguem pertinentes.

Atenciosamente,

DocuSigned by:
Marcelo Takeyama
6014FFDCF2F6469...

Associação Brasileira das Empresas de Cartões de Crédito e Serviços - ABECS

DocuSigned by:
Luís Vicente Magni De Cicco
90648D5D0B4C4BD...

DocuSigned by:
Carolina Sansão Moreira Alexandrino
9AC4593ECAF84A4...

Federação Brasileira de Bancos - FEBRABAN

ESTUDO PRELIMINAR

Anonimização e Pseudonimização para a proteção de dados pessoais

Autoridade Nacional de Proteção de Dados

Diretor-Presidente
Waldemar Gonçalves Ortunho Junior

Diretores
Arthur Pereira Sabbat

Joacil Basilio Rael

Miriam Wimmer

Equipe de elaboração

Albert França Josuá Costa

Diego Carvalho Machado

Fabíola de Gabriel Soares Pinto

Jeferson Dias Barbosa

Katia Adriana Cardoso de Oliveira

Mariana Talouki

Paulo Cesar dos Santos

Rodrigo Santana dos Santos

Versão 1.0	Dezembro/ 2023

Sumário

1. APRESENTAÇÃO

1. A Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), com o objetivo de definir fundamentos e promover a cultura de proteção de dados no Brasil, faz menção a processos que, mediante diferentes técnicas, possibilitam de algum modo afetar a vinculação do dado pessoal, de forma direta ou indireta, com o indivíduo, como as utilizadas em processos de anonimização e de pseudonimização.
2. A Autoridade Nacional de Proteção de Dados (ANPD), na perspectiva de estabelecer um ambiente normativo e orientativo para a proteção de dados, recebeu a autorização legal do § 3º do art. 12, da LGPD para dispor sobre essas técnicas, na forma de orientação aos agentes de tratamento de dados pessoais no Brasil.
3. A ANPD, em sua missão central de salvaguardar a privacidade e a proteção dos dados pessoais, com base em estudos técnicos desenvolvidos internamente[1], elaborou orientações e esclarecimentos sobre o tema, por entender que um melhor conhecimento sobre o processo e as técnicas de anonimização e pseudonimização é importante para que os agentes de tratamento adotem abordagens mais robustas de proteção de dados.
4. Alinhada a esse entendimento, a ANPD oferece este estudo preliminar com o intuito de disseminar os processos e as práticas de anonimização e pseudonimização, não só entre os agentes de tratamento, como também entre os titulares de dados pessoais, reforçando o seu compromisso em ser um parceiro ativo na construção de uma cultura de proteção de dados pessoais sólida e responsável no Brasil.
5. Quanto à **estrutura**, o estudo preliminar está organizado com a seguinte estrutura:
    - **Conceitos básicos** | Apresentação dos conceitos basilares, a partir de um glossário, e uma introdução geral ao regramento da anonimização e pseudonimização de dados de acordo com a disciplina normativa daLGPD.
    - **Os processos de anonimização e pseudonimização de dados na LGPD** | Análise dos processos de anonimização e pseudonimização de dados e seus aspectos jurídicos e técnicos, ressaltando a importância da avaliação contextual, o tipo de tratamento a ser realizado, o volume dos dados pessoais tratados e os riscos de reidentificação envolvidos para tomar a decisão de qual ou quais técnicas devem ser adotadas.
    - **Considerações finais** | Apontamento dos aspectos conclusivos e recomendações sobre os processos de anonimização e pseudonimização de dados à luz da LGPD.
    - **Apêndices** | Elementos complementares compostos de síntese geral, caderno com técnicas mais relevantes, suas caraterísticas, aplicações e estudos de caso.

6. Devido ao surgimento de novas técnicas e padrões, esta primeira versão tratará do tema observando, nesse contexto, a possibilidade de atualizações com base na evolução tecnológica.
7. Assim, a ANPD observará a evolução sobre o tema com o objetivo de atualização deste estudo preliminar, à medida que novas técnicas e novos entendimentos forem estabelecidos. Ademais, sugestões também podem ser enviadas para a Ouvidoria da ANPD, por meio da Plataforma Fala.BR (https://falabr.cgu.gov.br/).

2. CONCEITOS BÁSICOS

8. Para que seja possível melhor compreender as orientações que se pretende passar, alguns termos são esclarecidos de forma a padronizar e entender o seu significado e sua utilização ao longo deste estudo preliminar.

2.1. GLOSSÁRIO

- **Agente de tratamento:** O controlador e o operador.
- **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.
- **Banco de dados:** Conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.
- **Conjunto de dados:** *Vide* Banco de dados.
- **Controlador:** Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.
- **Dado anonimizado:** Dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.
- **Dado auxiliar**: identificador adicional empregado para vincular um dado pessoal, que passou por um processo de pseudonimização, e que é capaz de permitir a reidentificação da pessoa natural.
- **Dado pseudonimizado:** Dado que 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.

  [COMENTÁRIO: Nesta definição do conceito de "dado pseudonimizado", nos parece válido realizar ajuste redacional para incluir também recurso adicional, além do dado auxiliar. Dessa forma, sugerimos o texto a seguir: "Dado pseudonimizado: Dado que perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de **recurso e/ou** informação adicional mantid~~o~~**os** separadamente pelo controlador em ambiente controlado e seguro."]

- **Dado em fluxo**: Dado gerado continuamente a uma alta taxa de velocidade, com

tamanho potencialmente infinito e necessidade de processamento imediato.

- **Dado pessoal:** Informação relacionada a pessoa natural identificada ou identificável.
- **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.
- **Equivalência de classe:** Subconjunto de um conjunto que contém todos os elementos com algum valor de atributo igual a todos os elementos.
- **Identificador direto:** Dado que, por si só, permite identificar unicamente uma pessoa natural.
- **Identificador indireto:** Dado que, por si só, não tem a capacidade de identificar uma pessoa natural, mas pode ser agregado ou vinculado a dados auxiliares para identificar uma pessoa natural.

- **Métrica base:** Valor definido para mensurar o risco de reidentificação calculado unicamente com base no próprio conjunto de dados, como, por exemplo, a Equivalência de Classe.
- **Métrica contextual:** Métrica derivada de uma métrica base, com a incorporação de elementos particulares
- **Operador:** Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.
- **Titular:** Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.
- **Tratamento:** Toda a 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.
- **Variável dependente do contexto:** Característica interna do agente de tratamento que pode afetar o cálculo do risco de reidentificação.

2.2. ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO DE DADOS NA LGPD

9. A LGPD tratou, em seu art. 5º, incisos III e XI, sobre a anonimização como um processo em que um agente de tratamento utiliza determinadas técnicas para desvincular, de forma direta ou indireta, o dado pessoal do seu titular por meio do uso de técnicas de processamento de dados.
10. A anonimização, conforme definido no art. 5º, XI, da Lei, é o processo por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, tornando-se, portanto, anonimizado.

11. Em consequência, o dado anonimizado surge, no estágio atual da tecnologia, como o resultado da implementação de processo de anonimização por agente de tratamento, em que são empregados meios técnicos razoáveis e disponíveis na ocasião do tratamento.

12. O dado anonimizado, conforme disposto no art. 5º, III, da LGPD, é aquele dado inicialmente vinculado à pessoa natural, mas que foi posteriormente submetido a processo de anonimização a partir de técnicas ou paradigmas, como generalização e privacidade diferencial. Em razão da remoção dos identificadores diretos e indiretos, os dados perdem, a princípio, o caráter pessoal.

13. Os conjuntos de dados podem conter identificadores que possibilitam a associação, direta ou indireta, a um indivíduo, nos termos do art. 5º, XI e art. 12, § 4º, da LGPD. Daí se dizer que os identificadores podem ser diretos ou indiretos.

14. **O Identificador direto** é o dado que por si só permite identificar unicamente uma pessoa natural, sem a necessidade de combiná-lo com dados de outras fontes. O típico identificador direto de um titular de dados é o seu nome completo. Outro exemplo é o número de inscrição no Cadastro de Pessoas Físicas (CPF), que é considerado número único e suficiente para identificação do cidadão nos bancos de dados de serviços públicos, nos termos da Lei nº 14.534/2023.

15. Já o **identificador indireto**, por sua vez, é considerado o dado que por si só não tem a capacidade de identificar alguém, mas pode ser agregado e vinculado a dados auxiliares para identificar uma pessoa natural, a exemplo da nacionalidade, da idade, da raça, do CEP da residência, das características fenotípicas, ou do endereço de IP que podem ser necessários para distinguir alguém. Também conhecidos como “quase-identificadores”, os identificadores indiretos se relacionam ao “fenômeno das ‘combinações únicas”, isto é, tendo em vista que os atributos dos quase-identificadores variam de pessoa a pessoa, a combinação pode se tornar suficientemente singular a um único indivíduo. Por exemplo, em um estudo publicado no ano 2000, demonstrou-se que 87% da população dos Estados Unidos da América possuía características provavelmente únicas com base apenas no CEP de cinco dígitos (*5-digit ZIP code*), gênero e data de nascimento.

16. Considerando que, para se anonimizar um dado pessoal, serão utilizados meios técnicos razoáveis e disponíveis no momento desse processo, existe o risco de que alguns processos de anonimização possam ser revertidos no futuro. As circunstâncias podem mudar com o tempo e novos desenvolvimentos tecnológicos e a disponibilidade de informações adicionais podem comprometer os processos de anonimização anteriores.

[COMENTÁRIO: Importante que a ANPD considere e destaque no texto que, ainda que a anonimização possa não reduzir a probabilidade de reidentificação de um titular a zero, tais técnicas, especialmente as baseadas nas melhores práticas, são relevantes e se mostram efetivas para de fato anonimizar dados pessoais. Importante mencionar que a probabilidade de reidentificação de um

titular, além de poder ser difícil de ser mensurada, não necessariamente compromete a anonimização, especialmente quando ocorre a utilização de técnicas eficazes de anonimização, de acordo com as melhores práticas, as quais devem ter um peso maior no processo ao invés de apenas se considerar riscos remotos e hipotéticos, até mesmo para não colocar a prática em descrédito. Caso a técnica de anonimização, considerando fatores e riscos concretos, possa ser revertida facilmente, estaria mais próxima da pseudonimização.]

A anonimização não reduz a probabilidade de reidentificação de um conjunto de dados a zero, isto é, a anonimização não elimina todo e qualquer risco de reidentificação de um conjunto de dados; o processo de anonimização e a forma como é implementado terão influência direta na probabilidade de reidentificação.

17. A reidentificação é o processo de tentar discernir os identificadores que foram removidos dos dados desidentificados, inclusive a partir de técnicas de anonimização de dados. Assim, a reidentificação pode transformar dados anonimizados em dados pessoais por meio do uso, por exemplo, de correspondência de dados ou técnicas semelhantes.

Dados anonimizados não são considerados dados pessoais

18. O**s dados anonimizados não são considerados dados pessoais**, por isso não estão sujeitos à proteção da LGPD, salvo quando o processo de anonimização a que foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

19. Já o termo **pseudonimização** não é o mesmo que **anonimização**, conforme define a LGPD no § 4º do seu art. 13:

Pseudonimização é o 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 (art. 13, § 4º, da LGPD).

20. Ou seja, a anonimização consiste na conversão de dados pessoais em dados que não podem ser usados para identificar qualquer indivíduo. Já no processo de pseudonimização, é necessário que o dado pessoal seja substituído por identificador ou informação adicional que permita fazer a vinculação entre o dadopseudonimizado e o dado pessoal do seu titular, observando que:

    a) essas informações adicionais devem ser mantidas separadamente dos dados pseudonimizados; e

    b) devem ser tomadas medidas técnicas e organizacionais de segurança da base de identificadores ou informações adicionais, para garantir que os dados pessoais não sejam atribuídos a um indivíduo.

21. Em diferentes disposições da LGPD há indicações para a aplicação de um dos processos de anonimização ou de pseudonimização. Durante e depois do tratamento dos dados, em situações específicas, no tratamento e utilização de dados pessoais, é aplicável um desses processos para garantir ao titular a proteção contra o uso indevido ou abusivo dos seus dados pessoais.

22. Há recomendação para uso da anonimização e da pseudonimização quando do tratamento de dados pessoais para realização de estudos por órgãos de pesquisa (art. 7º, IV) e no campo da saúde pública (art. 13, *caput*), em casos em que o controlador deseja conservar os dados para uso posterior e como um direito que o titular de dados possui, respectivamente, podendo requerer do controlador a anonimização de seus dados pessoais, quando esta é viável.

[COMENTÁRIO: Destacamos que o trecho "e como um direito que o titular de dados possui, respectivamente, podendo requerer do controlador a anonimização de seus dados pessoais, quando esta é viável" parece remeter ao art. 18, IV, da LGPD, que versa sobre os direitos dos titulares. Importante ressaltar que, caso a referência seja de fato a esse artigo, a anonimização é cabível apenas se os dados forem desnecessários, excessivos ou tratados em desconformidade com a LGPD, e não mediante simples requerimento do titular em qualquer situação, quando a anonimização for viável.]

Situações e Aplicação das técnicas na LGPD	**Processo**
Condicionante para o tratamento nas hipóteses do uso dos dados pessoais e dados pessoais sensíveis em pesquisas – art. 7º, inciso IV; art. 11, alínea "c" do inciso II;	Anonimização
Reversão do processo de anonimização – art. 12, *caput* e §§ 1º e 3º;	Anonimização
Tratamento de dados sensíveis – estudos e pesquisas em saúde pública – art. 13, *caput* e § 4º.	Pseudonimização
Conservação dos dados após o término do tratamento – *caput* no art. 16, incisos II e IV;	Anonimização
Direito dos titulares no art. 18, inciso IV; **compartilhamento e da portabilidade de dados** - § 6º e 7º do art. 18.	Anonimização

[COMENTÁRIO: Em relação à tabela acima, sugere-se algumas alterações para melhor esclarecimento:
- O título pode ser alterado para "Situações e recomendações de aplicação das técnicas na LGPD", considerando que não é necessariamente vinculante.
- Em relação à primeira linha ("Condicionante para o tratamento..."): O art.7º, IV, e o art. 11, alínea "c" do inciso II, da LGPD, preveem que a anonimização será garantida sempre que possível, isto é, o artigo não insere a anonimização como uma condicionante para o tratamento de dados para realização de pesquisas. Portanto, sugere-se a alteração do trecho para incluir: "Sempre que possível, no tratamento nas hipóteses do uso dos dados pessoais e dados pessoais sensíveis em pesquisas - art.7º, inciso IV; art.11, alínea "c" do inciso II;".
- Em relação à terceira linha ("Tratamento de dados sensíveis..."): O caput do art. 13 também traz a possibilidade de anonimização, além da pseudoanonimização, em caso de estudos e pesquisas de saúde pública. Assim, sugerimos a complementação da tabela com referida informação, inlcuindo "Pseudonomização ou Anonimização" na coluna de "Processo".
- Em relação à quarta linha ("Conservação dos dados..."): Sugere-se manter no exemplo apenas a menção ao inciso "IV", pois o art.16, II, menciona a anonimização como uma possibilidade e não como uma regra diferentemente do inciso IV.]

3. OS PROCESSOS DE ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO DE DADOS

23. Os dados pessoais, quando submetidos a processos de anonimização e pseudonimização, passam por alterações que visam a impedir sua associação direta ou indireta a um indivíduo específico. A distinção crucial entre dados anonimizados e pseudonimizados reside na reversibilidade do processo e na capacidade de reestabelecer a associação com a identidade original do indivíduo.

24. No caso do processo de anonimização, os dados são modificados de tal forma que se reduz substancialmente o risco de vinculá-los novamente a pessoa natural identificada ou identificável, mesmo com o uso de dados auxiliares. A remoção dos identificadores mediante esse processo torna tais dados como não pessoais para qualquer entidade, inclusive para o controlador dos dados.

    [COMENTÁRIO: Sugere-se retirar o trecho "mesmo com o uso de dados auxiliares". Considerando que o dado passa por um processo de anonimização, não caberia o uso de dados auxiliares para identificá-lo, pois estes só são aplicáveis ao processo de pseudonimização. Quando um dado pessoal passar pelo processo de anonimização, ele sequer conseguirá ser vinculado a um dado auxiliar.]

25. Já na pseudonimização, embora a associação direta seja inicialmente obscurecida, existe a possibilidade de reverter esse processo mediante o uso de informações adicionais mantidas separadamente pelo controlador em um ambiente controlado e seguro. Essas informações adicionais, sob controle estrito, são essenciais para reestabelecer a ligação entre os dados pseudonimizados e a identidade do titular de dados.

26. Ambos os processos buscam atender aos preceitos de proteção da privacidade e de proteção dos dados pessoais. Contudo, a pseudonimização, por permitir a reversibilidade do processo pelo controlador, demanda uma gestão cuidadosa das informações adicionais utilizadas para essa finalidade. É crucial que essas informações sejam mantidas em um ambiente seguro e controlado, evitando qualquer possibilidade de acesso não autorizado que possa comprometer a privacidade dos titulares de dados. Dessa forma, a escolha entre anonimização e pseudonimização dependerá da necessidade de preservação da privacidade e da reversibilidade dos dados no contexto específico de tratamento, considerando a finalidade, a utilidade dos dados e os riscos envolvidos no processo.

3.1. ASPECTOS JURÍDICOS RELEVANTES

3.1.1 Anonimização e os princípios de proteção de dados pessoais

27. A partir da análise do art. 12, *caput*, da LGPD, compreende-se que a utilização de meios técnicos na anonimização de dados consiste, na verdade, em um conjunto de atos ou medidas entre si relacionadas que fazem parte de um **processo**. Dessa forma, a anonimização se desenvolve em uma série de etapas que se inicia com o processamento de dados pessoais e tem o objetivo de, com a aplicação de técnicas variadas, desassociar identificadores do dado em seu estado originário ou bruto.

28. O objetivo da anonimização é afetar os **identificadores** presentes em um dado, ou conjunto de dados, porque esses são os elementos informativos que "mantém relação particularmente privilegiada e próxima com certo indivíduo." Os identificadores podem ser diretos ou indiretos, como já mencionado anteriormente.

29. Na análise sobre a anonimização, é importante considerar uma premissa adotada pelo regime de proteção de dados pessoais brasileiro[9]: consistindo a anonimização de dados em um processo de remoção de identificadores diretos e indiretos, os dados pessoais submetidos ao processo de anonimização devem ser, na origem, objeto de legítimo tratamento pelo agente responsável.[10]

30. Tal afirmação possui desdobramentos relevantes. Primeiramente, fica evidenciado que o ato inicial do processo de anonimização configura operação de tratamento de dado pessoal, atraindo, assim, a aplicação de princípios e regras da LGPD. O segundo desdobramento é o de que a anonimização não é capaz de *per se* legitimar atividade de tratamento originalmente ilícita por falta de hipótese legal que lhe dê fundamento.

[COMENTÁRIO: Sugere-se a exclusão do trecho que se refere ao primeiro desdobramento. O processo de anonimização não deve ser entendido estritamente como operação de tratamento de dado pessoal sujeita às regras previstas na LGPD (por ex.: o processo de anonimização dos dados não está sujeito ao atendimento de uma finalidade específica ou, ainda, à necesisdade de atribuição de base legal). Na realidade, o que deveria importar na anonimização é a origem lícita dos dados pessoais coletados, não havendo necessidade de observar a LGPD no processo de anonimização. Inclusive, neste sentido, o Considerando/Recital 26 da GDPR, menciona que a lei não é aplicável aos dados pessoais tornados anônimos, "*The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.***"**

Além disso, a anonimização em si, considerando dados coletados legitimamente, é um instrumento de proteção à privacidade que pode ser usado, inclusive, quando encerram-se hipóteses de tratamento que justificam a manutenção dos dados pessoais. De maneira geral, atrair todo o ônus regulatório para a anonimização representa custo e esforço injustificáveis, que oneram o controlador e não representa, de fato, uma proteção adicional ao titular.]

31. Em outras palavras, se todo tratamento de dado pessoal deve ser legitimado por ter suporte normativo em hipótese legal estabelecida previamente, como as previstas nos artigos 7º e 11 da LGPD, a anonimização pressupõe tratamento lícito, pois não é processo capaz de transformar em legítima a irregular atividade de tratamento de dados sem fundamentação legal.

Por exemplo, num contexto de emergência sanitária, um controlador que fornece aplicativo móvel de edição de imagem e texto começa a coletar dados de geolocalização dos dispositivos de seus usuários sem qualquer hipótese legal que legitime sua atividade. Não será eventual anonimização de dados que removerá a ilicitude do tratamento; tais dados deverão, portanto, ser eliminados e o tratamento, interrompido.

32. Sendo assim, por se tratar o ato inicial do processo de anonimização uma operação de tratamento de dado pessoal, deve-se levar em consideração os princípios e regras de proteção de dados pessoais aplicáveis, **em especial os princípios da finalidade, adequação e necessidade.**

[COMENTÁRIO: Sugere-se a alteração desse trecho, conforme comentário do item 30, a fim de esclarecer que embora a anonimização não caracterize operação de tratamento de dado pessoal, as operações de tratamento de dados pessoais que antecedem o processo de anonimização (por ex.: coleta, armazenamento, etc.) devem estar alinhados a determinados princípios da LGPD.]

33. O **princípio da finalidade** estabelece que o tratamento de dados pessoais deverá ser realizado em consonância com propósitos legítimos, explícitos, específicos e informados ao titular quando da operação de tratamento de dados pessoais.

34. É o que prescreve o art. 6º, I, da LGPD. Isso significa que, para a realização da anonimização de acordo com o regime geral de proteção de dados, deve o controlador informar com clareza que uma das finalidades da coleta dos dados pessoais é a futura anonimização.

[COMENTÁRIO: Sugerimos a exclusão ou revisão dos itens 34 ao 40, pois uma vez que a anonimização descaracteriza o dado pessoal como tal, e, portanto, não atraindo a aplicação da LGPD sobre o dado anonimizado, entendemos não haver razão para as disposições que constam em referidos itens, inclusive pelo fato da utilização da anonimização para manutenção dos dados para uso exclusivo pelo controlador ser uma das hipóteses trazidas pela própria LGPD (inciso IV, art. 16).

Entendemos que a "anonimização" é um "meio" para atingir uma determinada finalidade, e não uma finalidade em si que precise ser destacada de forma específica, como indicado no Guia.

35. Entretanto, se a finalidade de anonimização não houver sido informada originalmente, a sua realização importará "tratamento posterior" ou uso secundário, que, necessariamente, deverá ser compatível com a finalidade inicialmente informada aos titulares dos dados.

36. Nessa linha, deve a anonimização, como tratamento posterior, observar o **princípio da adequação**, que, por sua vez, determina que a licitude da operação de tratamento depende da sua compatibilidade com a(s) finalidade(s)legítima(s),

específica(s) e explicitamente informada(s) ao titular dos dados, levando-se em consideração o contexto em que se realiza o tratamento.

37. De maneira semelhante ao que já foi objeto de recomendação no "Guia Orientativo – Tratamento de dados pessoais pelo Poder Público", a avaliação da compatibilidade da anonimização de dados com a(s) finalidade(s) originária(s) deve ter em consideração, por exemplo:

    I. o contexto da atividade de tratamento de dado pessoais, riscos envolvidos e outras circunstâncias relevantes do caso concreto;

    II. a existência de conexão fática ou jurídica entre a finalidade original e os objetivos do processo de anonimização; e

    III. as expectativas legítimas dos titulares e os possíveis impactos do tratamento posterior sobre seus direitos.

38. O **princípio da necessidade** é outra norma de alta relevância para a anonimização de dados. De acordo com o art. 6º, III, o tratamento de dados pessoais deverá ser limitado ao mínimo necessário para a realização de suas finalidades, abrangendo apenas os "dados pertinentes, proporcionais e não excessivos em relação às finalidades" especificadas.

39. A necessidade do tratamento da informação exige uma avaliação preliminar direcionada a verificar se o propósito especificado pode ser alcançado com o uso mínimo de dados pessoais ou com métodos idôneos a reduzir ou eliminar seus identificadores. Dessa forma, uma vez cumprida a finalidade para a qual certos dados pessoais foram coletados, a retenção dos dados para exclusivo uso do controlador será possível desde que, à luz do princípio da necessidade, os dados sejam anonimizados.

    [COMENTÁRIO: Importante pontuar que não existe vedação para o uso secundário/posterior de dados pessoais, desde que sustentados por hipótese legal válida e cumprido os demais requisitos.

    De qualquer forma, vale ressaltar que não há se falar na observância do princípio da necessidade para uso exclusivo do controlador quando este anonimizará os dados, em razão da inaplicabilidade da LGPD neste caso. Assim, sugerimos a exclusão indicada no final do parágrafo para que não haja confusão interpretativa do Estudo: "~~Dessa forma, uma vez cumprida a finalidade para a qual certos dados pessoais foram coletados, a retenção dos dados para exclusivo uso do controlador será possível desde que, à luz do princípio da necessidade, os dados sejam anonimizados.~~"]

40. Ainda nesse sentido, importa chamar atenção ao fato de que *"a anonimização não é uma medida de segurança impositiva, que deve ser adotada em todo e qualquer tratamento de dados pessoais"*. A pertinência da adoção do processode anonimização decorre de um juízo de necessidade à luz da(s) finalidade(s) especificada(s) para o tratamento de dados na situação concreta.

3.1.2 Riscos de reidentificação de dados anonimizados

41. O processo de anonimização se desenvolve por meio da utilização de técnicas diversificadas (ver Apêndices II e III) cuja pertinência é justificada de acordo com as características e outros aspectos contextuais do banco de dados que o agente de tratamento pretende anonimizar. Isso porque, além de a LGPD não impor o uso de técnicas de anonimização específicas, não há qualquer metodologia universalmente aplicável.

42. De acordo com o atual estado da arte, pode-se afirmar a existência de um consenso científico sobre a impraticabilidade de um cenário de ausência de risco de reidentificação nas situações de tratamento de dados anonimizados. Tendo em vista o enorme volume de dados auxiliares disponibilizados publicamente na internet e o desenvolvimento da capacidade de processamento e análise de algoritmos de reidentificação, é fundada a afirmativa de que sempre haverá fatores de risco de reidentificação.

[COMENTÁRIO: Pelo Guia, a definição de "dado auxiliar" está atrelada ao processo de pseudonimização, considerando-o como um *"identificador adicional empregado para vincular um dado pessoal, que passou por um processo de pseudonimização, e que é capaz de permitir a reidentificação da pessoa natural"*, isto é, pela definição, o dado auxiliar aparenta ser uma espécie de "id" que possibilitaria o dado pseudoanonimizado ser reindentificado após uma pseudononimização. No mais, o dado auxiliar não aparenta ser um dado disponibilizado publicamente na internet, sugere-se a exclusão do trecho final.

Além disso, reiteramos os nossos comentários ao item 16 desse guia, com relação à possibilidade de reidentificação e da robustez dos processos de anonimização.

43. Nesse sentido, a adoção de **modelo baseado em riscos** relacionado à identificabilidade de dados, a partir dos meios e esforços suscetíveis de serem razoavelmente utilizados, também se mostra pertinente na avaliação da robustez do processo de anonimização. Tal avaliação não pode ser episódica ou pontual, mas sim iterativa e contínua, visto que novos riscos podem advir ao longo do tempo na medida dos avanços tecnológicos e da quantidade de dados auxiliares disponíveis, por exemplo.

44. Os riscos de reidentificação de dados anonimizados são expressos, em linguagem técnica, como possíveis **ataques de reidentificação**. O termo "ataque" é tomado por empréstimo da literatura especializada em segurança computacional, em que a avaliação do nível de segurança de determinado sistema computacional ou algoritmo de cifragem ocorre a partir do uso da figura de um hipotético "atacante" que possui certas habilidades, conhecimento ou acesso. "Uma avaliação de risco envolve a catalogação da variedade de potenciais atacantes, e, para cada um, a probabilidade de sucesso".

45. Cumpre ressaltar que essa noção de "atacante" não se confunde com aqueles sujeitos que praticam crimes ou atos antijurídicos. Basta considerar o exemplo de pesquisadores que avaliam a robustez de base de dados anonimizada

compartilhada publicamente frente a certos algoritmos de reidentificação com o uso de dados auxiliares disponibilizados em bases de acesso público.

46. Alguns exemplos de ataques ou riscos de reidentificação que podem ser mencionados são:

    I. a distinção;
    II. a possibilidade de ligação; e
    III. a inferência.

47. A distinção consiste na possibilidade de se isolar alguns ou todos os registros que destacam um indivíduo numa base de dados. A possibilidade de ligação é definida pela capacidade de se estabelecer uma conexão entre pelo menos dois registros relativos ao mesmo indivíduo ou ao mesmo grupo de pessoas. Já o risco de inferência diz respeito à possibilidade de inferir, com uma significativa probabilidade, o valor de um atributo a partir dos valores de um conjunto de outros atributos.

3.1.3 As noções de "esforços razoáveis" e "meios próprios"

48. A compreensão do processo de anonimização e dos critérios a serem considerados para avaliar os riscos de reidentificação, requer, necessariamente, a interpretação de dois termos previstos no artigo 12 da LGPD: "esforços razoáveis" e "meios próprios".

[COMENTÁRIO: Importante que sejam definidos ao menos alguns parâmetros mais objetivos relacionados aos conceitos de "esforços razoáveis" e "meios próprios".]

49. O primeiro configura um **conceito jurídico indeterminado** normativo, ou seja, um conceito em larga medida incerto em seu conteúdo e extensão, dependente de preenchimento valorativo pelo aplicador do Direito. Em termos práticos, isso significa que a ANPD, como intérprete e aplicadora da LGPD, deve preencher, com elementos e critérios pertinentes com o caso concreto, a noção de "esforços razoáveis", dentro do sentido literal possível e em coesão com o contexto significativo da lei, que, aliás, prevê no § 1º do art. 12, relevantes parâmetros interpretativos.

50. A LGPD estabelece no art. 12, § 1º, um **rol exemplificativo** de aspectos objetivos que devem ser avaliados pelo intérprete ao preencher (ou determinar), nas situações concretas, o conteúdo do que é esforço razoável, isto é, dos meios suscetíveis de ser razoavelmente utilizados. Conforme o texto da lei, *"a determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios".*

51. Na análise dos fatores **custo e tempo** necessários para a possibilidade de reidentificação dos titulares e reversão do processo de anonimização, deve se considerar, por exemplo, os encargos derivados da força de trabalho e recursos humanos, custos econômicos e tempo de dedicação exigidos para se alcançar a reidentificação. Neste sentido, a ANPD já teve a oportunidade de se manifestar

em Nota Técnica elaborada no caso envolvendo o tratamento de microdados pelo Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (INEP):

> "*A avaliação relativa à eventual reversão dos dados e aos seus impactos deve se basear em evidências e em cenários que considerem aspectos objetivos da realidade. Afastam-se, assim, análises meramente especulativas, baseadas em cenários irreais, de difícil ou improvável ocorrência ou, ainda, que desconsiderem limitações práticas, decorrentes de custos muito elevados ou de meios técnicos de disponibilidade restrita.*"

[COMENTÁRIO: Esse trecho destacado pela ANPD é relevante e deve ser mantido, pois não se deve levar em conta "*análises meramente especulativas, baseadas em cenários irreais, de difícil ou improvável ocorrência ou, ainda, que desconsiderem limitações práticas, decorrentes de custos muito elevados ou de meios técnicos de disponibilidade restrita.*"]

52. Outros fatores objetivos importantes para a compreensão dos esforços razoáveis para reidentificação ou reversibilidade do processo de anonimização são **as tecnologias e técnicas disponíveis** ao tempo das operações de tratamento e a **licitude** dos meios utilizados. Este último fator implica dizer que a prática de crimes cibernéticos ou o uso de meios proibidos por lei configuram meios e esforços irrazoáveis para a reidentificação ou reversão do processo de anonimização.

53. Diferentemente da noção de "esforços razoáveis", o conceito de **meios próprios** tem conteúdo mais delimitado, podendo-se afirmar que são **meios próprios** as habilidades, os dados, instrumentos e técnicas disponíveis ao próprio agente de tratamento responsável pela anonimização. Sendo assim, importa ressaltar que, a partir do texto normativo do art. 12, *caput*, da LGPD, compreende-se que a avaliação da possibilidade de reidentificação de dados e a reversão do processo de anonimização devem ter em consideração não apenas o uso de meios próprios do agente de tratamento responsável pela anonimização, mas também a atuação de outras pessoas ou entidades que, com meios e esforços razoáveis, podem reidentificar conjunto de dados anonimizados.

3.2. O PROCESSO DE ANONIMIZAÇÃO

54. Os dados pessoais podem ser tratados em diversos formatos, tais como tabular, imagem, áudio e vídeo. Cada um desses formatos apresenta diferentes características que devem ser abordadas por técnicas de anonimização distintas. Por esse motivo, o agente de tratamento não deve considerar a anonimização de forma restrita às técnicas, mas considerar uma abordagem mais ampla baseada em processo, em que as técnicas de anonimização são elementos que compõem o todo.

55. Convém ressaltar que os dados que tenham sido tornados irreversivelmente anonimizados deixam de ser considerados "dados pessoais" e o processamento desses dados não exige conformidade com a legislação de proteção de dados.

Isso implica que as organizações podem utilizá-los para finalidades, desde que compatíveis, que vão além daquelas para as quais foram originalmente coletados e esses dados podem ser mantidos indefinidamente.

[COMENTÁRIO: Vide nossos comentários sobre os itens 34 a 40 deste guia. Uma vez que o dado anonimizado não é considerado dado pessoal, a LGPD não é aplicável e não se exige conformidade com a norma. Assim, os dados anonimizados podem ser tratado para finalidades além das originais, pois o seu uso não está restrito ao disposto na LGPD.Não há necessidade de que os dados anonimizados sejam usados para finalidades "(...) desde que compatíveis, que vão além daquelas para as quais foram originalmente coletados (...)". Assim, sugere-se excluir o trecho "desde que compatíveis", deixando claro que não há limitação no uso desses dados do ponto de vista da LGPD, posto que inaplicável, especialmente limitação em relação à finalidade.]

56. O processo de anonimização, orientado por uma abordagem baseada em riscos, tem como objetivo fornecer um conjunto mínimo de etapas que podem servir de guia de boas práticas aos agentes de tratamentos de dados. Essas etapas sugerem que o agente identifique e compreenda os riscos envolvidos em sua atividade, bem como adote medidas para mitigá-los.

57. A discussão do processo de anonimização é iniciada com a apresentação do conflito entre a utilidade e o grau de anonimização do dado pessoal, seguida por uma importante ponderação sobre a gestão do risco de reidentificação de dados anonimizados por meio de um processo de anonimização baseado em risco.

[COMENTÁRIO: Sugere-se incluir outros fatores na discussão do processo de anonimização, inclusive o seu custo, técnicas e esforços necessários. "A discussão do processo de anonimização é iniciada com a apresentação do conflito entre a utilidade e o grau de anonimização do dado pessoal, seguida por uma importante ponderação sobre a gestão do risco de reidentificação de dados anonimizados por meio de um processo de anonimização baseado em risco, bem como outros fatores, como a viabilidade, custos, técnicas e esforços necessários para realizar a anonimização ou a reidentificação."]

58. Dentro do âmbito das técnicas de anonimização, este documento apresenta no Apêndice II um caderno com o objetivo de elucidar em quais cenários, contextos e para qual formato de dado cada técnica abordada se mostra mais adequada. Adicionalmente, são apresentadas suas aplicações e limitações, fornecendo aos responsáveis pela anonimização informações para uma análise criteriosa com o objetivo de identificar a melhor abordagem de acordo com as características específicas e considerações de segurança e privacidade aplicáveis.

3.2.1 Utilidade dos dados pessoais derivada da finalidade da operação de tratamento

[COMENTÁRIO: Vide os nossos comentários aos itens 34 ao 40. No mais, entendemos que vale haver uma distinção no intuito de que a abordagem de risco seja aplicável para utilização da técnica de anonimização sob o ponto de vista da segurança conquanto a possibilidade de reidentificação do titular por terceiro, tendo em vista a evolução tecnológica, e não visando que um dado seja "meio anonimizado", a fim de ter utilidade

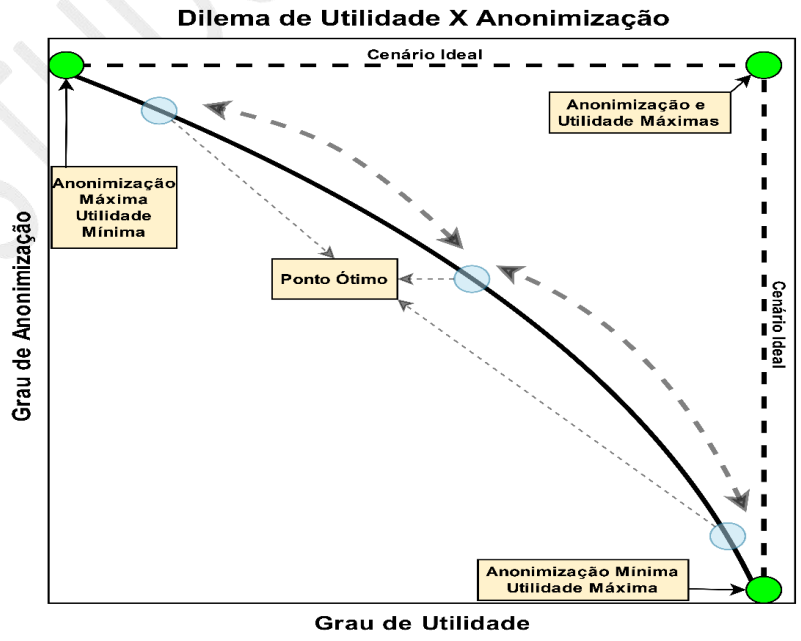
para o controlador na qualidade de dado pessoal, o que, a nosso ver, é possível extrair do texto, pois a própria LGPD dispõe que "os dados anonimizados não serão considerados dados pessoais para os fins desta Lei" (art. 12, caput). Além disso, idealmente, as técnicas consideradas mais seguras para anonimização poderiam ser indicadas no guia.]

59. A LGPD determina que os dados pessoais devem ser tratados para propósitos legítimos, específicos, explícitos e informados ao titular. Partindo desse enunciado, é possível observar que a atividade de tratamento de dados pessoais precisa estar atrelada a uma finalidade específica, de tal forma que compete ao agente de tratamento identificar o grau de utilidade do dado pessoal para alcançar a finalidade especificada, e em consequência estabelecer o grau necessário de anonimização dos dados.

> **Anonimização não torna os dados inúteis** - um processo adequado de anonimização mantém os dados funcionais para um determinado propósito de tratamento e finalidades específicas.

60. Em termos teóricos, existe um ponto ótimo em que o grau de utilidade do dado pessoal e o grau de anonimização são simultaneamente máximos. Entretanto, em termos práticos esse ponto ótimo não é fácil de ser alcançado, pois depende de um ajuste fino entre duas variáveis conflitantes. Conforme exposto na Figura 1, o ponto ótimo encontra-se em um ponto entre os dois extremos do dilema.

Figura 1: Dilema Utilidade x Anonimização.



Fonte: Elaboração própria.

61. De tal forma, a abordagem da anonimização como um processo contínuo baseado em risco possibilita que o agente de tratamento defina, de acordo com seu contexto, o compromisso entre o grau de utilidade e o grau de anonimização que contemple a finalidade definida no tratamento e minimize o risco de reidentificação do titular.

3.2.2 Gestão do risco de reidentificação

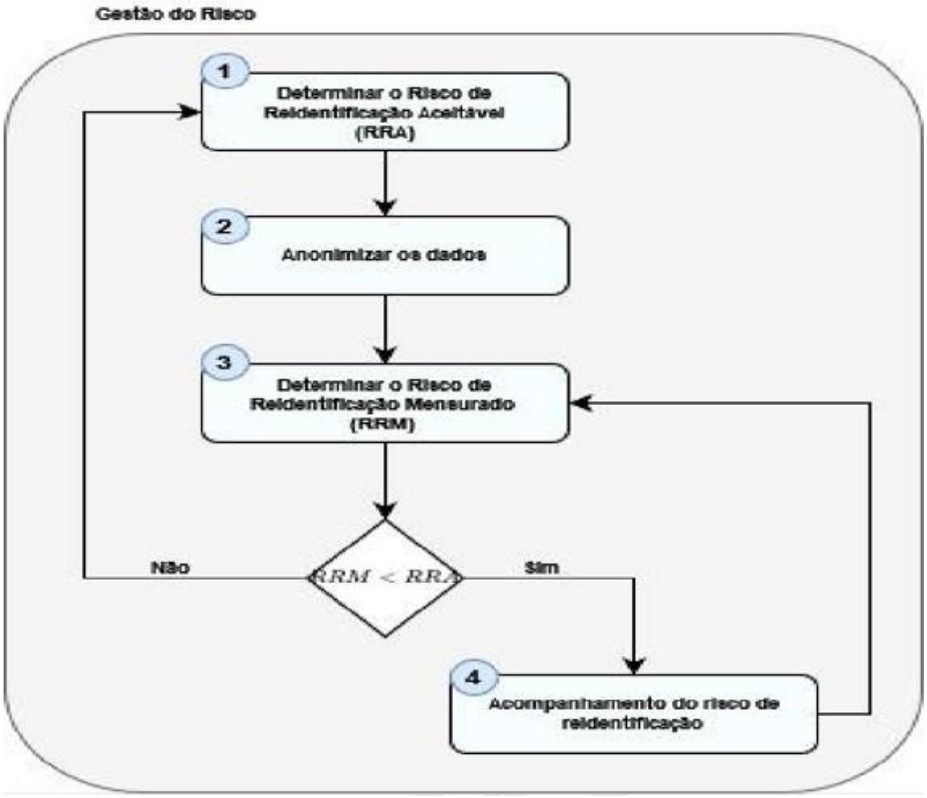
62. O processo de anonimização de dados pessoais não deve ser entendido como um processo definitivo, em que os dados após a anonimização apresentam risco zero de reidentificação. Corroborando com essa ideia, não há técnica de anonimização com eficácia plena, tendo todas elas um risco de reidentificação associado, cabendo ao agente de tratamento gerenciar esse risco com a adoção de um processo de anonimização adequado.

63. O processo tem como objetivo minimizar os riscos de reidentificação mantendo a utilidade dos dados tratados. Para isso, a gestão do risco de reidentificação deve ser realizada de forma contínua durante todo o tratamento dos dados, permitindo que o agente de tratamento tenha evidências suficientes para a tomada de decisão relacionada à proteção de dados e à privacidade dos titulares.

64. O cenário de anonimização apresenta características que podem variar para a realidade de cada agente de tratamento. Por esse motivo, a anonimização não deve se restringir à discussão de técnicas, mas sim uma abordagem mais ampla baseada em processo. Nesse contexto, este estudo preliminar apresenta uma proposta de processo de anonimização baseado em risco, com 4 etapas, que pode ser adaptado às necessidades de cada agente de tratamento (Figura 2).

[COMENTÁRIO: A proposta apresentada do processo de anonimização é válida, porém, não deve ser considerada como a única e não deve ser vinculante.]

Figura 2: Processo de anonimização baseado em risco.



Fonte: Elaboração própria.

65. A **primeira etapa** consiste na determinação do **Risco de Reidentificação Aceitável** (RRA) para um certo conjunto de dados, e tem como objetivo estipular um limite superior para o risco. Um risco de reidentificação superior ao limite estabelecido descaracterizará o conjunto de dados como anonimizado.
[COMENTÁRIO: O conjunto de dados com risco de reidentificação superior a ponto de descaracterizar, concretamente, a anonimização, poderia, a depender do contexto, tratar-se de dado pseudonimizado. De qualquer forma, importante pontuar que não havendo metodologia padronizada, pode-se ter diferentes análises sobre a adequação do RRA.]

66. Essa primeira etapa é de extrema importância e possui uma gama de variáveis dependentes do contexto que devem ser observadas pelo agente de tratamento. Desse modo, não é possível estabelecer uma metodologia padronizada a todos os casos, cabendo ao agente de tratamento definir o risco de reidentificação aceitável para os dados tratados.

67. Pode-se citar como exemplos de variáveis de contexto a existência de dados pessoais sensíveis ou dados financeiros que podem diminuir o limite do risco aceitável.
[COMENTÁRIO: Entendemos que a mera existência de dados financeiros não afeta o risco de identificação aceitável e não deveriam ser considerados para diminuir o limite de risco aceitável. Inclusive, os dados financeiros, especialmente por si só, não são aptos a identificar um titular. Dessa forma, sugerimos excluir dados financeiros do trecho a seguir: "Pode-se citar como exemplos de variáveis de contexto a existência de dados pessoais sensíveis ~~ou dados financeiros~~ que podem diminuir o limite do risco aceitável.**"]**

68. A **segunda etapa** consiste na aplicação do conjunto de técnicas de anonimização escolhido. O objetivo dessa etapa é produzir um conjunto de dados anonimizados que tenha um risco de reidentificação não superior ao limite do risco aceitável definido na etapa anterior. A escolha das técnicas de anonimização deve levar em consideração as características dos dados.

69. A **terceira etapa** consiste em definir o Risco de Reidentificação Mensurado (RRM) de um ataque de reidentificação ter sucesso no conjunto de dados, pós-anonimização; o RRM preferencialmente deve assumir a forma de probabilidade.

70. De modo semelhante à primeira etapa, variáveis dependentes do contexto podem ser observadas pelo agente de tratamento, como exemplo tem-se a condição do conjunto de dados ser público, compartilhado ou privado. Essa condição pode afetar o risco real de reidentificação.

71. Considerando a diversidade de natureza, escopo, contexto e finalidade de cada tratamento realizado pelo agente de tratamento, não é possível definir uma métrica única para a mensuração do risco de reidentificação. Por tal razão, este Guia adota a expressão **Métrica Contextual** para se referir à métrica utilizada para mensurar o RRM de acordo com a realidade de cada agente de tratamento.

72. É importante destacar que para dados textuais estruturados há algumas métricas de mensuração de risco bem conhecidas, tais como a K-Anonimização, T-Proximidade e L-Diversidade. Essas métricas derivam de uma métrica base que utiliza o conceito de equivalência de classe da teoria dos conjuntos para determinar o risco de reidentificação. Inclusive, a K-Anonimização é exemplificada no Apêndice III.

73. A métrica de risco de reidentificação pode ser computada para cada um dos titulares pertencentes ao conjunto de dados, e os valores resultantes podem ser ponderados, por exemplo, com a média aritmética, para determinar o valor geral da métrica contextual. Por fim, o valor geral da métrica contextual pode ser então ponderado pelas variáveis contextuais, resultando no Risco de Reidentificação Mensurado.

$$\textbf{\textit{Risco de Reidentificação Mensurado}} = \boldsymbol{\theta} * \boldsymbol{V_C}$$

74. $\boldsymbol{\theta}$ representa o valor geral da métrica contextual e $\boldsymbol{V_C}$ representa um fator de ponderação das variáveis contextuais, quando existentes, caso não existam $\boldsymbol{V_C}$ pode assumir o valor de 1.
75. Por exemplo, no contexto de base de dados públicas ou compartilhadas, o risco deve ser majorado e, consequentemente, o valor de V_C deve ser definido de forma adequada a representar a majoração do risco.
76. O Risco de Reidentificação Mensurado (RRM) deve ser comparado ao Risco de Reidentificação Aceitável (RRA). Caso o RRM seja maior do que o RRA, o conjunto de dados não apresenta a condição de estar anonimizado, sendo necessário o reinício do processo de anonimização. Caso contrário, é necessário acompanhar o uso do conjunto de dados, especialmente quando operações realizadas sobre ele possam modificar o risco mensurado, tais como operações de inclusão, alteração ou deleção de dados; havendo essas operações é necessário atualizaro nível do risco mensurado.

[COMENTÁRIO: Idealmente, se o objetivo do processo de anonimização baseada em risco é comparar o risco aceitável de reidentificação com o risco de reidentificação mensurado, as técnicas precisam ser minimamente equivalentes ou comparáveis, para viabilizar um grau de comparação de valores compatíveis entre si.]

3.3. O PROCESSO DE PSEUDONIMIZAÇÃO

77. A pseudonimização de dados pessoais significa substituir quaisquer características identificáveis dos dados por um pseudônimo, ou seja, um valor que não permite a identificação direta do titular dos dados. A LGPD define a pseudonimização como o tratamento de dados pessoais de forma que esses dados não possam mais ser atribuídos a um titular de dados específico sem o uso

de informações adicionais, desde que:

a) essas informações adicionais sejam mantidas separadamente; e
b) estejam sujeitas a medidas técnicas e organizacionais para garantir que os dados pessoais não sejam atribuídos a um indivíduo identificado ou identificável.

78. Embora a pseudonimização tenha diversas utilidades, é importante distingui-la da anonimização, já que aquela oferece apenas uma proteção limitada à identidade dos titulares em muitos casos, permitindo ainda a identificação por meio de métodos indiretos. Quando se utiliza um pseudônimo, a depender da técnica utilizada, é possível identificar o titular por meio da análise dos dados subjacentes ou relacionados, o que deve ser tratado com atenção à luz dos princípios da LGPD.

79. Em certos casos, a natureza dos dados, o contexto em que são utilizados ou o propósito da coleta e retenção podem tornar a anonimização eficazmente impossível. Mesmo nessas circunstâncias, as organizações podem optar por empregar técnicas de anonimização ou pseudonimização com as seguintes finalidades, de acordo com a LGPD:
    a) Como parte de uma estratégia de "privacidade desde a concepção" (*privacy by design*) destinada a oferecer uma proteção adicional aos titulares dos dados;
    b) Como parte de uma estratégia de minimização de riscos ao compartilhar dados com operadores ou outros controladores de dados;
    c) Para evitar violações acidentais quando a equipe tem acesso a informações pessoais; e
    d) Como parte de uma estratégia de "minimização de dados" voltada a reduzir os riscos de violações de dados para os titulares dos dados.

[COMENTÁRIO: A anonimização pressupõe a inaplicabilidade da LGPD, portanto, não há que se falar em empregar técnicas de anonimização com finalidades de acordo com a LGPD. Neste sentido, o Considerando/Recital 26 da GDPR, menciona que a GDPR não é aplicável aos dados anônimos, "*The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable*." Sugere-se alterar a redação para: "Ainda, se aplicável, as organizações podem optar por empregar técnicas de pseudonimização com as seguintes finalidades, de acordo com a LGPD".]

80. Vale ressaltar que, mesmo após a anonimização, persistem alguns riscos inerentes e que a pseudonimização não é equivalente à anonimização, uma vez que as informações ainda mantêm sua característica de dados pessoais.

81. A Lei Geral de Proteção de Dados Pessoais não indica técnicas de pseudonimização específicas, mas estabelece princípios e requisitos gerais para o tratamento de dados pessoais.

82. No entanto, a pseudonimização é um conceito amplamente reconhecido na LGPD e é encorajada como uma medida de proteção de dados. Algumas técnicas de pseudonimização em conformidade com a LGPD podem ser:

a) **Substituição de Dados:** nesta técnica, dados pessoais são substituídos por pseudônimos ou códigos, tornando-os menos identificáveis. Por exemplo, um número de CPF pode ser substituído por um código alfanumérico único.

b) **Ofuscação de Dados:** envolve a transformação de dados pessoais de forma que sejam mais difíceis de identificar. Isso pode incluir o embaralhamento de informações ou a substituição de valores de dados por outros valores semelhantes.

c) **Tokenização:** envolve a substituição de dados pessoais por tokens ou códigos que não têm significado fora do contexto do sistema. Esses tokens podem ser usados para fins de identificação, mas não revelam as informações reais dos titulares de dados.

d) **Cifração:** técnica que converte dados em um formato criptografado que só pode ser decifrado com uma chave. Isso torna os dados pessoais ilegíveis para qualquer pessoa sem acesso à chave correspondente.

e) **Mascaramento de Dados:** envolve a ocultação parcial de informações, revelando apenas uma parte dos dados e ocultando o restante. Por exemplo, um número de telefone pode ser mascarado como "(XX) XXXX-1234", mostrando apenas os últimos dígitos.

f) **Salting:** técnica é comumente usada na criptografia de senhas. Um valor aleatório (chamado de "salt") é adicionado aos dados antes da encriptação, tornando os pseudônimos únicos e mais seguros contra-ataques de força bruta.

Criptografia típica não é anonimização – Criptografia é uma técnica de pseudonimização. Como a informação original precisa estar acessível, as transformações aplicadas pelos algoritmos criptográficos são projetadas para serem reversíveis, no que é conhecido como descriptografia. Entretanto, vários algoritmos criptográficos (simétricos, assimétricos e de hash) podem realizar processamentos unidirecionais. Nesses casos atendem os requisitos da anonimização, desde que os dados cifrados sejam úteis.

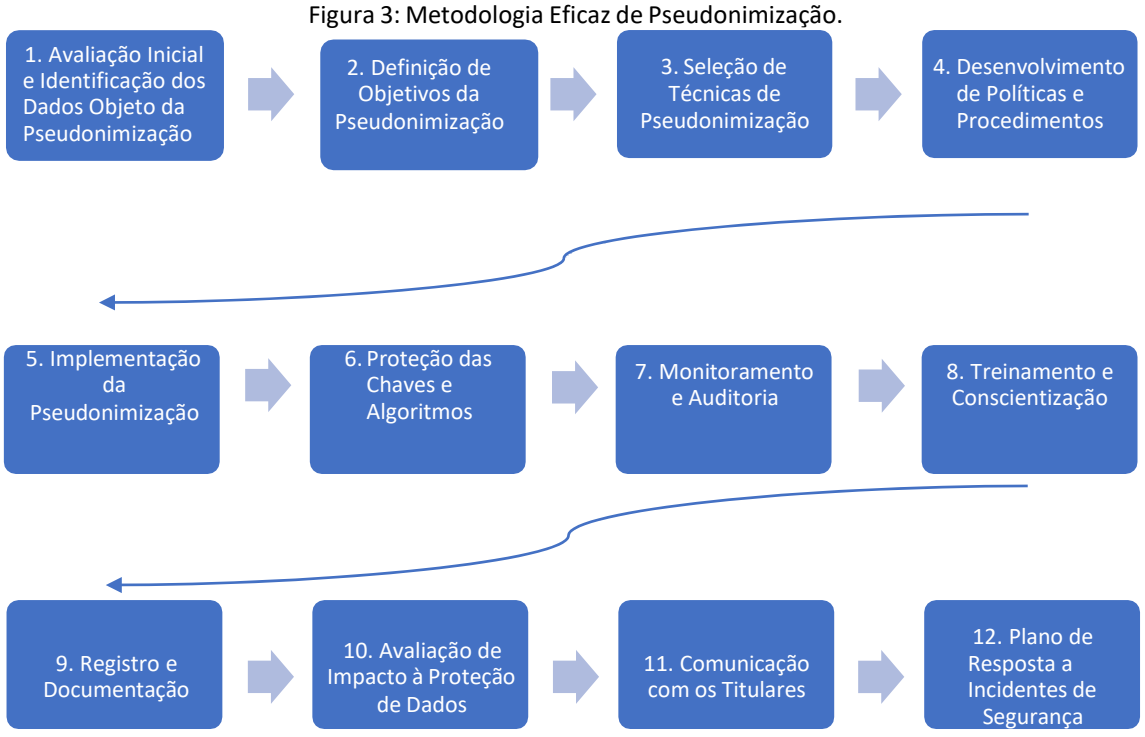
[COMENTÁRIO: Sugerimos alguns ajustes redacionais no destaque acima: "Criptografia ~~típica~~ **pode ou** não ~~é~~ **ser** anonimização – ~~Criptografia é uma técnica de pseudonimização. Como~~ **Diante d**a informação original ~~precisa~~ estar acessível, as transformações aplicadas pelos algoritmos criptográficos são projetadas para serem reversíveis, no que é conhecido como descriptografia. **Neste cenário a Criptografia é uma técnica de pseudonimização.** Entretanto, vários algoritmos criptográficos (simétricos, assimétricos e de hash) podem realizar processamentos unidirecionais. Nesses casos atendem os requisitos da anonimização, desde que os dados cifrados sejam úteis."]

83. É importante observar que a LGPD enfatiza que, para que a pseudonimização seja

eficaz, as informações adicionais que permitem a reversão da pseudonimização (por exemplo, as chaves criptográficas) devem ser mantidas separadamente e protegidas por medidas técnicas e organizacionais adequadas. Além disso, a LGPD enfatiza a importância de garantir a privacidade e a segurança dos dados pessoais em todas as etapas do tratamento. Portanto, a escolha da técnica de pseudonimização deve ser feita com cuidado, levando em consideração o contexto, os riscos associados e a sensibilidade dos dados.

84. Desenvolver uma metodologia eficaz de pseudonimização de dados pessoais, alinhada com as melhores práticas de mercado e em conformidade com os princípios da LGPD é fundamental para garantir a privacidade e a segurança das informações pessoais.
[COMENTÁRIO: A metodologia apresentada do processo de pseudonimização de dados é válida, porém, não deve ser considerada como a única e não deve ser vinculante. Além disso, a pseudonimização dos dados, assim como a anonimização, não é medida obrigatória a ser usada em todos os casos e a sua não utilização não compromete a licitude do tratamento dos dados que não estejam anonimizados ou pseudonimizados, desde que o tratamento seja efetuado de acordo com a LGPD.]

Figura 3: Metodologia Eficaz de Pseudonimização.



84. Conforme ilustração acima (Figura 3), para o desenvolvimento dessa metodologia algumas etapas devem ser observadas:

1. Avaliação Inicial e Identificação dos Dados Objeto da Pseudonimização: inicie com uma avaliação abrangente de quais dados pessoais serão coletados e tratados. Identifique quais dados pessoais serão objeto da pseudonimização, considerando os riscos e o tratamento realizado, dando ênfase a dados considerados sensíveis, como por exemplo, dados de saúde, origem racial ou étnica, convicção religiosa, opinião política, entre outros.

2. Definição de Objetivos da Pseudonimização: estabeleça claramente os objetivos da pseudonimização, incluindo a proteção da privacidade do titular dos dados, a redução do risco de violações de dados e o cumprimento da LGPD.

3. Seleção de Técnicas de Pseudonimização: escolha as técnicas de pseudonimização apropriadas com base na natureza dos dados. Isso pode incluir o mascaramento de informações pessoais, o uso de tokenização, o embaralhamento de dados ou a criptografia, dentre outros. A escolha dependerádas características específicas dos dados e dos riscos associados.

4. Desenvolvimento de Políticas e Procedimentos: crie políticas e procedimentos claros para garantir a pseudonimização adequada. Isso inclui diretrizes sobre como realizar a pseudonimização, armazenar chaves criptográficas de forma segura e garantir a rastreabilidade e o acesso somente a pessoal autorizado.

5. Implementação da Pseudonimização: implemente as técnicas de pseudonimização de acordo com as políticas e procedimentos estabelecidos. Certifique-se de que todos os dados pessoais sejam adequadamente pseudonimizados antes de serem armazenados ou processados. Em alguns casos, técnicas diferentes podem ser aplicadas, concomitantemente, para produzir uma pseudonimização eficiente.

6. Proteção das Chaves e Algoritmos: garanta que as chaves e algoritmos utilizados no processo de pseudonimização, como por exemplo, chaves criptográficas, senhas de acesso a sistemas ou a arquivos, códigos-fonte, dentre outros, sejam armazenadas de forma segura e acessíveis apenas a pessoal autorizado. Os registros de auditoria devem ser mantidos, documentando quando as chaves foram usadas, quem as utilizou e com que finalidade. Isso é valioso para conformidade regulatória, registro de operações e investigações de segurança. É fundamental garantir que os dados possam ser revertidos quando necessário de forma segura, pelo controlador.

Como uma boa prática para o gerenciamento de chaves, técnicas como a implementação de logs de eventos e sistemas de monitoramento podem ser empregados para facilitar a rastreabilidade no uso das chaves, e ainda, as chaves podem ser armazenadas de forma segura usando práticas como a criptografia de

chaves mestras e Módulos de Segurançaem Hardware (HSMs).

[COMENTÁRIO: O processo de pseudonimização estará sempre atrelado a um tratamento de dados pessoais, isto é, terá uma finalidade definida, um registro de tratamento etc., portanto, não visualizamos a necessidade de novos registros de auditoria do tratamento pelo mero fato de ocorrer pseudonimização dos dados. No mais, não é necessariamente factível visualizar finalidade de acessos às informações por meio de registros de logs. Das etapas descritas, entendemos que as indicadas nos itens 7 a 12 abaixo são etapas aplicáveis em contexto amplo e geral do tratamento de dados pessoais, não sendo o caso de uma exigência específica ao processo de pseudonimização.]

7. Monitoramento e Auditoria: implemente sistemas de monitoramento e auditoria para verificar continuamente a eficácia da pseudonimização e garantir o cumprimento das políticas e procedimentos. Realize revisões e auditorias regulares a fim de acompanhar as mudanças regulatórias, tecnológicas e melhores práticas de mercado relacionadas à pseudonimização e ajuste sua metodologia conforme necessário.

8. Treinamento e Conscientização: forneça treinamento regular aos colaboradores que lidam com dados pessoais para garantir que compreendam a importância da pseudonimização e saibam como aplicá-la corretamente.

9. Registro e Documentação: mantenha registros detalhados de todas as atividades de pseudonimização, incluindo datas, técnicas utilizadas, responsáveis e propósitos. Isso é importante para fins de prestação de contas, rastreabilidade e registro de operações.

10. Avaliação de Impacto à Proteção de Dados: realize a avaliação de impacto sobre a proteção de dados, elaborando o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) quando apropriado, a fim de avaliar os riscos associados à pseudonimização e garantir a conformidade com a LGPD. Considere a elaboração do RIPD sempre que o tratamento envolver alto risco.

11. Comunicação com os Titulares: esteja preparado para informar de forma transparente e acessível aos titulares sobre a pseudonimização e os direitos de acesso e correção de suas informações pessoais, conforme exigido pela LGPD.

[COMENTÁRIO: Nos parece que informar ao titular sobre a existência ou não de pseudonimização em um tratamento de dados específico, excede o princípio da transparência, considerando que, além de não ser razoável ou viável, também pode vir a revelar segredos comerciais e industriais. Ademais, a nosso ver, a pseudonimização se caracteriza como uma medida de segurança, não trazendo a informação a respeito dela benefícios para o titular, uma vez que a LGPD seria aplicável e, portanto, os seus aspectos precisariam ser observados. Assim, sugerimos a exclusão desse trecho ou mesmo uma adequação, no intuito de não criar a obrigatoriedade de informação sobre a pseudonimização. Nos parece que, inclusive, essa pode ser uma técnica mutável dentro do tratamento de dados, que pode ou não ser definida desde o começo deste, mas que não necessariamente influenciaria nos direitos do titular.]

12. Plano de resposta a Incidentes de Segurança: desenvolva um plano de resposta a incidentes de segurança com dados pessoais que inclua procedimentos para lidar, entre outras situações, com acessos não autorizados e tratamentos inadequados ou ilícitos, incluindo as ações de mitigação apropriadas para reverter ou mitigar os efeitos dos prejuízos gerados.

[COMENTÁRIO: Ainda que a metodologia indicada para o processo de pseudonimização seja exemplificativa, nos parece válido retirar este ponto, considerando que o Plano de Respostas de incidentes de uma empresa é único e pode não haver segregação específica nos casos de pseudonimização. Ademais, esse item reflete genericamente os princípios da LGPD voltados para a segurança dos dados do titular, assim entendemos que não agrega e poderia ser excluído.]

4. CONSIDERAÇÕES FINAIS

85. Com a publicação do presente estudo preliminar, a ANPD pretende manter sua postura estratégica de promover na sociedade brasileira maior efetividade do regime de proteção de dados pessoais, fornecendo esclarecimentos e orientações em linha com o atual contexto socioeconômico e tecnológico do país.
86. Busca-se orientar os agentes de tratamento sobre a anonimização e pseudonimização de dados como processos contínuos com base em abordagem de riscos, e não somente limitar-se à indicação de aplicação de técnicas. Assim, esclarece-se que, dada a velocidade do progresso tecnológico, disponibilização de dados auxiliares e sofisticação de possíveis ataques, torna-se necessário manter a segurança e o cuidado com os processos.
87. Nos processos de anonimização e pseudonimização não existe uma solução única que se adeque a todas as organizações. Na maioria dos casos, não é possível fornecer recomendações mínimas de parâmetros a serem usados e cada organização deve, portanto, utilizar os mecanismos e técnicas que sejam apropriadas para as suas circunstâncias.
88. O presente documento não objetiva esgotar o tema da anonimização e pseudonimização no contexto da proteção de dados. Ao contrário, lança as bases para a expansão das orientações da ANPD para fortalecer a cultura e a proteção de dados pessoais. Sendo assim, contamos com as colaborações e sugestões sobre questões importantes que, porventura, não tenham sido tratadas ou que precisem de mais esclarecimentos.

5. REFERÊNCIAS

AGGARWAL, Charu C.; YU, Philip S. A general Survey of Privacy-Preserving Data Mining Models and Algorithms. Privacy-Preserving Data Mining. Advances in Database System. vol 34. Springer. 2008.

AEPD-EDPS, AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS – *European Data Protection Supervisor. Misunderstandings Related to Anonymization*. Disponível em: <https://edps.europa.eu/data-protection/our-work/publications/papers/aepd-edps-joint-paper-10-misunderstandings-related_en

AEPD-EDPS, AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS - European Data Protection Supervisor. *Orientaciones y garantias en los procedimentos de anonimización de datos personales.* [S.l.]. AEPD, 2016.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

BRASIL. Lei nº 9.784, de 29 de janeiro de 1999, que regula o processo administrativo no âmbito da Administração Pública Federal. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9784.htm.

BRASIL. Lei nº 14.534, de 11 de janeiro de 2023. Altera a Lei nº 7.116, de 29 de agosto de 1983, 9.454, de 7 de abril de 1997, a Lei nº 13.444, de 11 de maio de 2017, e Lei nº 13.460, de 26 de junho de 2017, para adotar número único para os documentos que especifica e para estabelecer o Cadastro de Pessoas Físicas (CPF) como número suficiente para identificação do cidadão nos bancos de dados de serviços públicos. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/lei/l14534.htm

_____AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Brasília: ANPD, versão 2.0., abr. 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_retificada.pdf

_____AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Portaria nº 1, de 8 de março de 2021. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-1-de-8-de-marco-de-2021-307463618

_____AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Resolução CD/ANPD nº 2, de 27 de janeiro de 2022; Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019#wrapper

_____AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Guia orientativo – Tratamento de dados pessoais pelo Poder Público. [S.l.]: ANPD, 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf

_____AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Nota Técnica nº 46/2022/CGF/ANPD. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/sei_00261-000730_2022_53-nt-46.pdf

_____AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-regulamento-de-dosimetria/Resolucaon4CDANPD24.02.2023.pdf

_____AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Guia Orientativo – Tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas. Brasília: ANPD, 2023.

DATA PROTECTION COMMISSION. *Guidance on Anonymisation and Pseudonymisation* [S.l.]: DPC, 2019. Disponível em: https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190614%20Anonymisation%20and%20Pseudonymisation.pdf

GARFINKEL, Simson L. *De-Identification of Personal Information*. [S.l.]: National Institute of Standards and Technology, 2015.

GRUPO DE TRABALHO DE PROTEÇÃO DE DADOS DO ARTIGO 29. *Opinion 4/2007 on the concept of personal data.* Bruxelas: [s. n.], 2007. Disponível em: https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf

GRUPO DE TRABALHO DE PROTEÇÃO DE DADOS DO ARTIGO 29. *Opinion 3/2013 on purpose limitation.* Bruxelas: [s. n.], 2013. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

GRUPO DE TRABALHO DE PROTEÇÃO DE DADOS DO ARTIGO 29. *Opinion 5/2014 on Anonymisation Techniques.* Bruxelas: [s. n.], 2014. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

LI N.; LI, T.; VENKATASUBRAMANIAN S. **T-Closeness: Privacy Beyond k-Anonymity and L-Diversity**. IEEE 23rd International Conference on Data Engineering, 2007.

SAMARATI, P.; SWEENEY. L. **Protecting privacy when disclosing information: k-anonymity and tis enforcement through generalization and suppression**. Technical Report, 1998.

SWEENEY, Latanya. *Simple Demographics Often Identify People Uniquely: Data Privacy Working Paper*. Pittsburgh: [s.n.], 2000. Disponível em: https://dataprivacylab.org/projects/identifiability/paper1.pdf

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados – RGPD). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679

6. APÊNDICES

[COMENTÁRIO: Reiteramos neste item "apêndices" os comentários sobre os tópicos correspondentes que já realizamos no restante do documento. Sugerimos que o texto dos apêndices seja adequado de acordo com as sugestões de texto e conceitos que realizamos acima.]

APÊNDICE I – PRINCIPAIS ESCLARECIMENTOS

a) **Dados anonimizados não são considerados dados pessoais**, por isso não estão sujeitos à proteção da LGPD, salvo quando o processo de anonimização a que foram submetidos for revertido, por algum meio eficaz.

b) A determinação do que seja **esforço razoável deve levar em consideração fatores objetivos, tais como o custo e o tempo necessários para reverter o processo** de anonimização, de acordo com as tecnologias disponíveis no momento da anonimização, e a utilização exclusiva de recursos tecnológicos próprios do agente de tratamento.

c) A anonimização de dados não é perpétua e indeterminada. **Existem riscos de que o processo de anonimização possa ser revertido no futuro**. As circunstâncias podem mudar com o tempo e os **novos desenvolvimentos tecnológicos e a disponibilidade de informações adicionais podem comprometer** os processos de anonimização anteriores.

d) Visando minimizar os possíveis impactos de um incidente de segurança, recomenda-se a **adoção de técnicas de pseudonimização e, quando cabível, a anonimização que busque a irreversibilidade, ou criem maior dificuldade de reidentificação**, desincentivando a tentativa de sua reversão.

e) **Pseudonimização não é o mesmo que anonimização -** pseudonimização é o 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 (art. 13, § 4º, da LGPD).

f) **Criptografia típica não é anonimização** - criptografia é uma técnica de pseudonimização. Como a informação original precisa estar acessível, as transformações aplicadas pelos algoritmos criptográficos são projetadas para serem reversíveis, no que é conhecido como descriptografia. Entretanto, vários algoritmos criptográficos (simétricos, assimétricos e de hash) podem realizar processamentos unidirecionais. Nesses casos atendem os requisitos da anonimização, desde que os dados cifrados sejam úteis.

g) **A anonimização dos dados pessoais nem sempre será possível** - nem sempre é possível reduzir o risco de reidentificação abaixo de um limite previamente definido, mantendo um conjunto de dados útil para um processamento ou finalidade específica.

h) **A anonimização não é para sempre** - existe o risco de que alguns processos de anonimização possam ser revertidos no futuro. As circunstâncias podem mudar com o tempo e novos desenvolvimentos tecnológicos e a disponibilidade de informações adicionais podem comprometer os processos de anonimização anteriores.

i) **A anonimização, geralmente, não reduz a probabilidade de reidentificação de um**

conjunto de dados a zero - a anonimização não impossibilita a reidentificação de um conjunto de dados; o processo de anonimização e a forma como é implementado terão influência direta na probabilidade de riscos de reidentificação.

j) **A anonimização não é um conceito binário e dependendo do processo utilizado pode ser medida** - é possível analisar e medir o grau de anonimização, por meio de técnicas usadas para garantir que o limite de risco de reidentificação não seja ultrapassado, como parte da metodologia de anonimização.

k) **A anonimização não deve ser totalmente automatizada -** ferramentas automatizadas podem ser usadas durante o processo de anonimização, no entanto, dada a importância do contexto e a avaliação geral do processo, poderá ser necessária a intervenção de um especialista humano.

[COMENTÁRIO: O processo de anonimização pode ser totalmente automatizado e é necessário para viabilizar a operação de grandes volumes. Considerando que alguns processos de anonimização podem utilizar exclusivamente processos automatizados sugere-se excluir esse trecho. Caso não seja possível, sugerimos alterar para "A anonimização poderá não ser totalmente automatizada", lembrando que a intervenção humana no processo é uma possibilidade, mas não uma obrigatoriedade, e que fica a critério do controlador.]

l) **Anonimização não torna os dados inúteis** - um processo adequado de anonimização mantém os dados funcionais para um determinado propósito de tratamento e finalidades específicas.

m) **Seguir um processo de anonimização que outros usaram com sucesso nem sempre levará a organização a resultados equivalentes** - seguir um caso de sucesso é um excelente ponto de partida, mas não é garantia de sucesso quando aplicado a outros casos.

n) Os **processos de anonimização precisam ser adaptados à natureza, escopo, contexto e finalidade do processamento -** bem como aos riscos e às variáveis probabilísticas e gravidade para os direitos e liberdades individuais.

o) **Existem riscos e interesses em reindentificar os dados anonimizados -** os dados pessoais têm um valor em si, para os próprios indivíduos e para terceiros. A reidentificação de um indivíduo pode ter um sério impacto sobre seus direitos e liberdades, assim a possibilidade de se reidentificar uma pessoa em um conjunto de dados, seja por curiosidade, por acaso ou motivado por um interesse real, como por exemplo, para pesquisa científica, fins jornalísticos ou atividade criminosa, não pode ser desconsiderada.

APÊNDICE II. CADERNO DE TÉCNICAS PARA ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO

01. Os dados pessoais anonimizados e pseudonimizados não possuem uma associação, direta ou indireta, a um indivíduo não sendo possível a sua identificação. A diferença primordial entre dados anonimizados e pseudonimizados se remete ao fato de que na pseudonimização essa associação pode ser reestabelecida pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro. Neste sentido, algumas técnicas que serão apresentadas podem ser empregadas tanto para a anonimização quanto para pseudonimização de dados pessoais. O que difere neste caso é a possibilidade de reversibilidade do processo pelo controlador com o uso de meios próprios e informações adicionais, mantidos sob o seu controle, na ocasião do tratamento. A seguir serão apresentadas algumas técnicas, exemplificativas e não exaustivas, para anonimização e pseudonimização de dados pessoais, textuais estruturados.

TÉCNICAS PARA ANONIMIZAR DADOS TEXTUAIS ESTRUTURADOS

Técnica de Adição de Ruído

Descrição

A técnica consiste em realizar pequenas modificações nos dados originais adicionando ruído nos dados. Normalmente utilizada em dados numéricos.

Exemplo

Dado original

Nome Completo				
FM				
AFB				
LB				
MTL				
CGG				
RJ				

Dado anonimizado por meio da adição de ruído.
Ao valor original é somando 1 desvio-padrão do intervalo de valores.
Para as colunas Idade e Quantidade filhos o valor do ruído foi trucando.

Nome Completo	Idade	Altura	Peso	Qtd. Filhos
FM	37	1,65	71,63	2
AFB	43	1,70	85,63	2
LB	27	1,90	110,63	0
MTL	29	1,78	70,63	1
CGG	37	1,62	71,63	2
RJ	43	1,70	85,63	2

Aplicação

Apropriada para dados numéricos em cenários em que a precisão dos dados não é essencial para o alcance da finalidade pretendida. A adição de ruído pode fazer com que o conjunto de dados perda suas propriedades estatísticas e o invalide para a finalidade pretendida.

Limites

- Aplicável preferencialmente em dados numéricos.
- Perda da precisão dos dados, a adição de ruído pode descaracterizar os dados com a perda de sua utilidade.
- Não deve ser utilizada quando a precisão dos dados é essencial.

Descrição

A técnica agrupa os dados com características em comum em um nível de granularidade maior. Os valores dos atributos são substituídos pelos valores do grupo.

Exemplo

Dado original

Nome Completo	Cidade de Nascimento	Idade
FM	Rio Branco	79
AFB	Macaíba	63
LB	Natal	91
MTL	Xapuri	85
CGG	Macaé	34
RJ	Rio de Janeiro	66

Dado anonimizado por meio da generalização

Nome Completo	Estado de Nascimento	Faixa Etária
FM	Acre	70-79
AFB	Rio Grande do Norte	60-69
LB	Rio Grande do Norte	90-99
MTL	Acre	80-89
CGG	Rio de Janeiro	30-39
RJ	Rio de Janeiro	60-69

Aplicação

Apropriada quando os dados possuem características em comum que permitem sua representação de forma generalizada, sem perda da utilidade.

Limites

- Aplicável somente a dados textuais estruturados.
- Aplicável somente em dados que compartilham características em comum.
- Não aplicável quando houver dados com valores únicos.
- Perda da precisão dos dados.
- Custo computacional elevado para aplicação em dados textos estruturados em fluxo

Técnica de Mascaramento

Descrição

A técnica consiste em substituir uma parte dos caracteres dos dados por um caractere símbolo (por exemplo * ou x).

Exemplo

Dado original

Nome Completo		Idade
FM		79
AFB		63
LB		91
MTL		85
CGG		34
RJ		66

Dado anonimizado por meio do mascaramento

Nome Completo	CPF	Idade
FM	***.111.111-**	79
AFB	***.222.222-**	63
LB	***.333.333-**	91
MTL	***.444.444-**	85
CGG	***.555.555-**	34
RJ	***.666.666-**	66

Aplicação

Apropriada quando a substituição de parte dos dados por um caractere simbólico fornece o nível desejado de anonimização, sem perda da utilidade.
No caso do CPF o mascaramento tem sido bastante aplicado, mas não deve ser empregado para qualquer finalidade ou qualquer contexto. Quando são substituídos cinco dígitos, a mascará obtida poderá ser válida para 100000 titulares de dados.

Limites

- Aplicável somente a dados textuais.
- Perda da precisão dos dados.
- Custo computacional elevado para aplicação em dados textuais estruturados em fluxo.

- Escolha do padrão adequado que permita desvincular o titular do dado anonimizado.
- Em casos de dados públicos ou compartilhados, como não há um padrão para o mascaramento, é possível que partes distintas dos dados estejam visíveis e por consequência os dados originais sejam reconstruídos.

Técnica de Permutação

Descrição

A técnica consiste em reorganizar os valores dos dados dentro do conjunto de dados, de tal forma que os valores originais ainda são representados, mas geralmente não mais associado ao seu titular.

Exemplo

Dado original

Nome Completo		Tempo de Profissão
FM		20
AFB		12
LB		15
MTL		8
CGG		25
RJ		12

Dado anonimizado por meio da permutação

Nome Completo	Profissão	Tempo de Profissão
FM	Advogado	15
AFB	Professor	20
LB	Enfermeiro	25
MTL	Vendedor	12
CGG	Médico Veterinário	12
RJ	Engenheiro de Software	8

Aplicação

Apropriada somente quando a análise dos dados precisa ser feita de forma agregada, pois a técnica elimina a possibilidade de analisar os dados ao nível do titular.

Limites

- Aplicável somente a dados textuais estruturados.
- Aplicável somente para análise agregada.
- Perda da precisão dos dados
- Custo computacional elevado para aplicação em dados textos estruturados em fluxo.

Técnica de Supressão

Descrição

A técnica consiste em excluir registros ou partes deles. A exclusão pode ser realizada em identificadores ou em partes dos registros.

Exemplo

Dado original

Nome Completo	Profissão	Tempo de Profissão
FM	Professor	20
AFB	Professor	12
LB	Professor	15
MTL	Professor	8
CGG	Enfermeiro	25
RJ	Professor	12

Dado anonimizado por meio da supressão.

Profissão	Tempo de Profissão
Professor	20
Professor	12
Professor	15
Professor	8
Professor	25

Aplicação

Apropriada somente quando a exclusão dos dados não afete a qualidade do tratamento a ser realizado ou o impossibilite. Registros com características únicas, isto é, com alto grau de unicidade, podem ser excluídos sem afetar a qualidade do conjunto de dados.

Limites

- A exclusão de registros pode afetar o conjunto de dados.
- Perda da informação excluída.

TÉCNICAS PARA ANONIMIZAR IMAGENS

Técnica de Desfoque Gaussiano (*blur*)

Descrição

A técnica consiste em aplicar um filtro de convolução nos *pixels* com o objetivo de desfocar uma área de interesse na imagem.

Dado Original	Dado Anonimizado com a técnica de desfoque gaussiano.
Aplicação Apropriada para dados de imagem ou vídeo em que se deseja desfocar regiões de interesse, em geral faces, para minimizar o risco de identificação do titular.	
Limites • Aplicável em dados de imagens ou frame de vídeo. • Dificuldade de definir o limite dos parâmetros do desfoque para garantir a utilidade do dado e ao mesmo tempo preservar a privacidade. • Dificuldade em identificar quais regiões da imagem o desfoque deve ser aplicado para garantir a utilidade do dado e ao mesmo tempo preservar a privacidade.	

Técnica de *Pixelização*

Descrição A técnica consiste diminuir a resolução da imagem, ou em uma área de interesse dessa para reduzir a nitidez da imagem.	
Dado Original	Dado Anonimizado com a técnica de *pixelização*.

Aplicação

Apropriada para dados de imagem ou vídeo em que se deseja *pixelização* regiões de interesse, em geral faces, para minimizar o risco de identificação do titular.

Limites

- Aplicável em dados de imagens ou frame de vídeo.
- Dificuldade de definir o limite dos parâmetros da *pixelização* para garantir a utilidade do dado e ao mesmo tempo preservar a privacidade.
- Dificuldade em identificar quais regiões da imagem a *pixelização* deve ser aplicada para garantir a utilidade do dado e ao mesmo tempo preservar a privacidade.

TÉCNICAS PARA PSEUDONIMIZAR DADOS TEXTUAIS ESTRUTURADOS

Técnica de Substituição por Contador

Descrição

A técnica consiste em substituir os identificadores por códigos únicos. É imprescindível que os códigos utilizados não se repitam para evitar ambiguidades e que os códigos não tenham relação com o identificador.

Exemplo

Dado original

Nome Completo	CPF	Idade
FM		79
AFB		63
LB		91
MTL		85
CGG		34
RJ		66

Dado pseudonimizado por meio de substituição por contador.

Nome Completo	CPF	Idade
FM	9000	79
AFB	9001	63
LB	9002	91
MTL	9003	85
CGG	9004	34
RJ	9005	66

Aplicação

Apropriada para conjunto de dados simples e possui fácil implementação.

Limites

- A escalabilidade da técnica para grandes conjuntos de dados é limitada.
- Necessidade de armazenar uma tabela auxiliar de mapeamento entre o identificador e o valor pseudonimizado.

Técnica de Função *Hash*

Descrição

A técnica consiste em aplicar uma função matemática que recebe como entrada o dado pessoal em sua forma original e o mapeia para um valor de saída na forma de um dado pseudonimizado. O dado de entrada pode ter um tamanho arbitrário e a função de mapeamento deve objetivar ser irreversível e livre de colisões.

Exemplo

Dado original

	Tempo de Profissão
	20
	12
	15
	8
	25
	12

Dado pseudonimizado por meio de função criptográfica

Nome Completo	Tempo de Profissão
965940fc76dd718d0000c10f964a31ab	20
5353c821d9b43ee6c394ab8cbdf007c4	12
fc1df2e704dbf009cb911d3a645fa6f0	15
b96ff5b76a82dc8e188964e2b66c1c93	8
c7aff31b290c0c21ac13a61f92cf7298	25
126a0eb057128bfc8b342507c1311aa4	12

Aplicação

A técnica contribui significativamente para a integridade dos dados, porém é considerada uma técnica sujeita à ataques de força bruta e de dicionário. Ambos os ataques consistem em testar as entradas possíveis para a função *hash* e verificar qual delas produz o valor *hash* (pseudonimizado) correspondente.

O ataque de força bruta testa todas as entradas possíveis, para *hashs* grandes desconsidera as colisões, tendo em vista a baixíssima probabilidade de ocorrência. Portanto, a força bruta somente é aplicável quando se conhece os candidatos aos dados em claro.

Por sua vez, o ataque de dicionário testa somente entradas pré-selecionadas, extraídas de um dicionário que contém as entradas com maior probabilidade de acerto.

Limites

- Sensível ao ataque de força bruta.
- Sensível ao ataque de dicionário.
- Necessidade de armazenar uma tabela auxiliar de mapeamento entre o identificador e o valor pseudonimizado.

Técnica de Encriptação

Descrição

A técnica consiste em converter os dados pessoais em um formato criptografado que só pode ser decifrado com a chave utilizada para criptografar, nos algoritmos simétricos, ou com a chave correspondente nos algoritmos assimétricos. A encriptação torna os dados pessoais ilegíveis sem o conhecimento da chave correspondente.

Exemplo

Dado original

Nome Completo	Tempo de Profissão
	20
	12
	15
	8
	25
	12

Dado pseudonimizado por meio de encriptação com chave de 128 bits.

Nome Completo	Tempo de Profissão
SzVEcrP6uX8yy1MaWSYC8Q==	20
lLAUoq0cWfkzTDN2+rddSQ==	12
EkLLOZImXFL2lzLzHCb9YQ==	15
Nvo1OFYnDKuZmQ56NNK5CQ==	8
NCXsMdEJUrIZmRVHszmiCQ==	25
iEl9JafMW0spZEFHRaxu7A==	12

Aplicação

A técnica de encriptação é uma técnica de pseudonimização considerada robusta e pode ser utilizada em bases de dados extensas, pois não depende de uma tabela auxiliar para o mapeamento entre o identificador e o valor pseudonimizado.

Limites

- Robustez depende do sigilo da chave utilizada para a encriptação e da chave correspondente para decriptação.

APÊNDICE III – TÉCNICAS DE MENSURAÇÃO DE RISCO PARA DADOS TEXTUAIS ESTRUTURADOS

K-ANONIMIZAÇÃO

01. A K-Anonimização é uma métrica de mensuração de risco de reidentificação para dados textuais estruturados derivada do conceito de equivalência de classe da teoria dos conjuntos. Apesar das limitações, é uma métrica de fácil compreensão e implementação.
02. Como parte do processo de anonimização, a K-Anonimização analisa se cada registro compartilha dados anonimizados com ao menos K-1 outros registros. Caso essa condição não seja alcançada, o conjunto de dados deve ser novamente anonimizado.
03. A Tabela 1 apresenta o conjunto de dados antes da anonimização que contém informações sobre funcionários de uma empresa. As técnicas de anonimização utilizadas são supressão, generalização e permutação. O valor definido para K é igual 2.

Tabela 1: Exemplo de conjunto de dados antes da anonimização.

Registro Profissional	Tempo de Serviço	Profissão	Gênero
3693	11	Engenheiro Civil	M
7807	28	Programador	M
6026	15	Encanador	M
0872	24	Eletricista	F
3164	20	Artífice	F
5190	19	Engenheiro Elétrico	F
4845	28	Programador	M
5867	22	Engenheiro de Software	M
9881	15	Encanador	M
3528	13	Engenheiro Civil	F
4442	21	Ajudante	F

04. A Tabela 2 apresenta o conjunto de dados após a anonimização considerando a métrica K-Anonimização com K = 2. Ao identificador Registro Profissional foi aplicada a técnica de supressão e para os identificadores Tempo de Serviço e Profissão foi aplicado a técnica de generalização. Por último, para o identificador Gênero foi aplicada a técnica de permutação
05. Os subconjuntos dos registros que compartilham os dados com ao menos um outro registro estão identificados por cores na Tabela 2.

Tabela 2 Exemplo de conjunto de dados após anonimização com valor de K = 2 para a K-Anonimização.

Tempo de Serviço	Profissão	Gênero
10 a 20	Obras	M
21 a 30	Tecnologia da Informação	F
10 a 20	Obras	M
21 a 30	Obras	F
10 a 20	Obras	M
10 a 20	Obras	M
21 a 30	Tecnologia da Informação	F
21 a 30	Tecnologia da Informação	F
10 a 20	Obras	M
10 a 20	Obras	M
21 a 30	Obras	F

APÊNDICE IV. ESTUDO DE CASOS

Caso 1: Dados agregados de localização – Supressão

01. A fim de adotar decisões informadas para combater emergência sanitária causada por epidemia de certa doença infectocontagiosa, a Secretaria Estadual de Saúde de um Estado-membro necessita de dados confiáveis a respeito da localização dos seus cidadãos. Os dados de localização são relevantes para que as autoridades estaduais do sistema de saúde pública possam identificar aglomerações de pessoas e, assim, orientarem-se para a implementação de medidas de prevenção, controle e fiscalização sanitárias de forma mais eficaz. A restrição ao ajuntamento das pessoas é medida importante para conter e diminuir o índice de contágio, além de identificar tendências de movimentação.
02. Com base na legislação instituidora de política pública de vigilância epidemiológica, discussões internas e consulta a especialistas, o governo estadual firmou acordo com os provedores de serviço de telefonia móvel A, B e C, para ter acesso a dados agregados de localização dos celulares dos respectivos usuários, com limites fixados à circunscrição territorial do Estado-membro e à duração da emergência sanitária.
03. Sendo assim, os provedores ou operadoras de telefonia móvel A, B e C compartilharam dados dos aparelhos de telefonia móvel conectados às Estações Rádio Base – ERBs. Cada aparelho de telefonia móvel envia para a ERB a que estão conectados a Identidade Internacional do Assinante Móvel (*Internation Mobile Subscriber Indentify* – IMSI) e a Identidade Internacional do Equipamento Móvel (*Internation Mobile Equipament Identify* – IMEI). Esses dados permitem que essas operadoras consigam identificar quais usuários estão conectados em quais ERBs em um determinado momento. Entretanto, para alcançar o objetivo da Secretaria Estadual de Saúde é necessário conhecer somente o quantitativo de usuários conectados em cada ERB em certo marco temporal.
04. Para resguardar a privacidade dos titulares de linhas móveis e atender ao interesse público, as operadoras de telefonia móvel, ao compartilharem os dados com a Secretaria de Saúde, aplicaram a técnica de supressão dos dados IMSI e IMEI, além de realizar a agregação do quantitativo de telefones móveis a fim de permitir o cálculo do índice de isolamento ou mapas de calor. Para tanto, consideraram-se: (i) o total de 21.641.000, o número de celulares somados os clientes das operadoras A, B e C no território do Estado; e (ii) a localização a partir das antenas (Estações Rádio Base – ERBs) às quais os dispositivos móveis estavam conectados.

Caso 2: Dados clínicos para pesquisa acadêmica – Supressão e Pseudonimização

01. Em estudo de dados clínicos de pacientes conduzido por grupo de pesquisadores de determinado Hospital das Clínicas de uma universidade federal, os dados relacionados à pressão arterial de 100 pacientes foram coletados nos atendimentos realizados com intervalo de 7 (sete) dias. Os dados coletados estão dispostos na Tabela 3.

Tabela 3. Dados coletados

Nome Completo	CPF	Endereço	Gênero	Idade	Peso	PD 1	PS1	PD 2	PS 2
Johanne Mendonça	111.111.111-11	Rua Norte, 372, Bairro A	M	51	113,30	13	9	15	7
Araci Coutinho Silva	222.222.222-22	Rua Leste, 122, Bairro A	F	46	48,50	10	6	12	9
Marcela Antunes	333.333.333-33	Rua dos Cocos, 7, Bairro B	F	37	97,44	10	7	11	7
Madruga Neves	444.444.444-44	Rua das Mangas, 22, Bairro B	M	41	59,28	14	7	11	8
Florinda Neves	555.555.555-55	Rua das Mangas, 22, Bairro B	F	58	54,30	11	7	11	7
Nilce Cavalcante	666.666.666-66	Rua Marte, 1, Bairro C	F	57	110,33	15	6	12	8
José Francisco	777.777.777-77	Rua Vênus, 36, Bairro C	M	73	58,55	18	10	17	10
Carmélia Andrade	888.888.888-88	Rua Vênus, 812, Bairro C	F	56	54,42	12	7	12	7
Andreia Priscila	999.999.999-99	Rua Sol, 12, Bairro C	F	35	109,38	17	10	16	9
...		...	...	...	...	...	...	...	...

02. Os pesquisadores submeteram esse conjunto de dados pessoais a processo de anonimização, tendo em vista que, conforme o desenho metodológico da pesquisa, a utilidade dos dados obtidos a partir da aplicação de certas técnicas de anonimização é preservada para os objetivos do estudo. Nesse sentido, foram aplicadas as técnicas expostas na Tabela 4.

03. Cumpre ressaltar, ainda, que os dados anonimizados serão mantidos em ambiente com controle de acesso e com pertinentes medidas de segurança previstas na política de segurança da informação do órgão de pesquisa.

Tabela 4. Técnicas utilizadas por Identificador.

Identificador	Técnica Utilizada	Descrição
Nome Completo	Supressão	Identificador direto é suprimido.
CPF	Pseudonimização	Substituição do CPF por um código único gerado.
Endereço	Supressão	O identificador é suprimido, pois não é útil para atender ao objetivo do tratamento.
Gênero		O processo de anonimização deve considerar a utilidade do dado para o tratamento desejado. No presente caso, os dados de gênero, peso, pressão diastólica 1, pressão sistólica 1, pressão diastólica 2 e pressão sistólica 2 estão correlacionados e essa correlação é útil para a finalidade da coleta de dados. Aplicação de técnicas de anonimização pode impactar na correlação dos dados e reduzir a utilidade deles.
Peso		O processo de anonimização deve considerar a utilidade do dado para o tratamento desejado. No presente caso, os dados de gênero, peso, pressão diastólica 1, pressão sistólica 1, pressão diastólica 2 e pressão sistólica 2 estão correlacionados e essa correlação é útil para a finalidade da coleta de dados. Aplicação de técnicas de anonimização pode impactar na correlação dos dados e reduzir a utilidade deles.
Pressão Diastólica 1		O processo de anonimização deve considerar a utilidade do dado para o tratamento desejado. No presente caso, os dados de gênero, peso, pressão diastólica 1, pressão sistólica 1, pressão diastólica 2 e pressão sistólica 2 estão correlacionados e essa correlação é útil para a finalidade da coleta de dados. Aplicação de técnicas de anonimização pode impactar na correlação dos dados e reduzir a utilidade deles.
Pressão Sistólica 1		O processo de anonimização deve considerar a utilidade do dado para o tratamento desejado. No presente caso, os dados de gênero, peso, pressão diastólica 1, pressão sistólica 1, pressão diastólica 2 e pressão sistólica 2 estão correlacionados e essa correlação é útil para a finalidade da coleta de dados. Aplicação de técnicas de anonimização pode impactar na correlação dos dados e reduzir a utilidade deles.
Pressão Diastólica 2		O processo de anonimização deve considerar a utilidade do dado para o tratamento desejado. No presente caso, os dados de gênero, peso, pressão diastólica 1, pressão sistólica 1, pressão diastólica 2 e pressão sistólica 2 estão correlacionados e essa correlação é útil para a finalidade da coleta de dados. Aplicação de técnicas de anonimização

		pode impactar na correlação dos dados e reduzir a utilidade deles.
Pressão Sistólica 2		O processo de anonimização deve considerar a utilidade do dado para o tratamento desejado. No presente caso, os dados de gênero, peso, pressão diastólica 1, pressão sistólica 1, pressão diastólica 2 e pressão sistólica 2 estão correlacionados e essa correlação é útil para a finalidade da coleta de dados. Aplicação de técnicas de anonimização pode impactar na correlação dos dados e reduzir a utilidade deles.

Caso 3: Compartilhamento de dados educacionais – Supressão, generalização, mascaramento, adição de ruídos e permutação.

01. A Secretaria Municipal de Educação da cidade de Privacinópolis precisa compartilhar os dados dos alunos matriculados com a Secretaria Municipal de Assistência Social com o objetivo da construção de relatórios sociais. Os dados estão dispostos na Tabela 5.

Tabela 5: Dados tratados

Nome Completo	Matrícula	Idade	Endereço	Gênero	Renda Familiar (R$)
Johanne Mendonça	2023010	7	Rua Norte, 372 – Bairro A	M	2188,44
Araci Coutinho Silva	2023011	10	Rua Leste, 122 – Bairro A	F	2195,82
Marcela Antunes	2023020	8	Rua dos Cocos, 7 - Bairro B	F	1947,20
Madruga Neves	2023021	9	Rua das Mangas, 22 - Bairro B	M	2014,38
Florinda Neves	2023022	11	Rua das Mangas, 22 - Bairro B	F	1942,34
Nilce Cavalcante	2023030	12	Rua Marte, 1 - Bairro C	F	1856,08
José Francisco	2023031	12	Rua Vênus, 36 - Bairro C	M	1835,86
Carmélia Andrade	2023032	8	Rua Vênus, 812 - Bairro C	F	1989,66
Andreia Priscila	2023033	10	Rua Sol, 12 - Bairro C	F	2082,96
Bruno da Costa	2023040	13	Rua Mercúrio, 36 - Bairro C	M	1911,34

02. Para tanto, se faz necessário conhecer o resumo dos dados tratados (Tabela 6):

Tabela 6: Descrição dos dados

Dado	Tipo	Dado Pessoal	Dado Pessoal Sensível	Identificador Direto	Descrição Estatística
Nome Completo	Qualitativo	S	N	S	Não Aplicável
Matrícula	Qualitativo	S	N	S	Não Aplicável
Idade	Quantitativo	S	N	N	Média: 10 Mediana: 10 Desvio-Padrão: 1,89
Endereço	Qualitativo	S	N	N	Não Aplicável
Gênero	Qualitativo	S	N	N	Moda: F Frequência M: 4/10 Frequência F: 6/10
Renda Familiar	Quantitativo	N	N	N	Média: R$ 1996,41 Mediana: R$ 1968,43 Desvio-Padrão: R$ 119,34 Mínimo: R$ 1835,85 Máximo: R$ 2195,82

03. Considerando o processo proposto neste estudo preliminar (Seção 3.2), há 4 etapas essenciais para a gestão do risco de reidentificação.

Determinar o Risco de Reidentificação Aceitável (RRA): É importante observar que a mensuração do risco de reidentificação é uma etapa que deve ser executada e gerenciada pelo agente de tratamento de acordo com o caso concreto, conforme sugerido no documento de Estudo Técnico sobre Anonimização de Dados na LGPD: Processo de Anonimização Baseado em Risco e Técnicas de Anonimização – Uma Introdução Computacional. No presente estudo de caso, nenhum dos dados tratados é considerado como sendo dado pessoal sensível e o compartilhamento dos dados é feito com outro órgão público por meios próprios. Entretanto, os dados são de crianças e adolescentes. De tal forma, o Risco de Reidentificação Aceitável (RRA) é definido em 0,35.

Anonimizar os dados: A Tabela 7**Erro! Fonte de referência não encontrada.** apresenta as técnicas utilizadas em cada um dos dados tratados. Por sua vez, a Tabela 8**Erro! Fonte de referência não encontrada.** apresenta o conjunto de dados após a aplicação do conjunto de técnicas de anonimização.

Tabela 7: Técnicas utilizadas por Identificador.

Identificador	Técnica Utilizada	Descrição
Nome Completo	Supressão	Identificador direto que será suprimido, a matrícula será utilizada.

Matrícula	Mascaramento	Os dois primeiro e o último digito será substituído por *.
Idade	Generalização	Os dados serão agrupados por duas faixas etárias. 1ª_ ≤ 10 e 2ª >10
Endereço	Generalização	Os dados serão agrupados pelo bairro do endereço.
Gênero	Permutação	Os valores serão trocados entre os gêneros, porém mantendo a frequência de cada gênero e a moda do conjunto de dados.
Renda Familiar	Adição de Ruído e Generalização	Cada valor individual será deslocado um desvio-padrão à direita e posteriormente generalizado em duas faixas de renda: ≤ R$ 2.000,00 e > R$ 2.000,00

Tabela 8: Identificadores após aplicação do conjunto de técnicas de anonimização.

Matrícula	Idade	Endereço	Gênero	Renda Familiar (R$)
**2301*	≤ 10	Bairro A	F	> 2.000,00
**2301*	≤ 10	Bairro A	M	> 2.000,00
**2302*	≤ 10	Bairro B	F	> 2.000,00
**2302*	≤ 10	Bairro B	F	> 2.000,00
**2302*	> 10	Bairro B	M	> 2.000,00
**2303*	> 10	Bairro C	F	≤ 2.000,00
**2303*	> 10	Bairro C	M	≤ 2.000,00
**2303*	≤ 10	Bairro C	F	> 2.000,00
**2303*	≤ 10	Bairro C	M	> 2.000,00
**2304*	> 10	Bairro C	F	> 2.000,00

Risco de Reidentificação Mensurado (RRM): O processo indica que após a aplicação do conjunto de técnicas de anonimização é necessário mensurar o risco de reidentificação utilizando alguma métrica contextual.

04. Nesse estudo, optou-se por utilizar a K-Anonimização, métrica derivada da equivalência de classe. Conforme sugerido no processo, a métrica deve ser computada para cada um dos identificadores e os valores resultados ponderados para determinar o valor geral do risco mensurado de reidentificação (Tabela 9).

Tabela 9: Risco Mensurado de Reidentificação.

Identificador	K-Anonimização por Classe do Identificador	K-Anonimização do Identificador (Média da K-Anonimização por Classe do Identificador)

Matrícula	**2301* = $\frac{1}{2}$ =0,50 **2302* = $\frac{1}{3}$ = 0,33 **2303* = $\frac{1}{4}$ = 0,25 **2304* = $\frac{1}{1}$ = 1,00	0,52
Idade	≤ 10 = $\frac{1}{6}$ = 0,16 > 10 = $\frac{1}{4}$ = 0,25	0,20
Endereço	Bairro A = $\frac{1}{2}$ = 0,50 Bairro B = $\frac{1}{3}$ = 0,33 Bairro C = $\frac{1}{5}$ = 0,20	0,34
Gênero	F = $\frac{1}{6}$ = 0,16 M = $\frac{1}{4}$ = 0,24	0,20
Renda Familiar (R$)	> 2.000,00 = $\frac{1}{8}$ = 0,12 ≤ 2.000,00 = $\frac{1}{2}$ = 0,50	0,31
Métrica Contextual (Média da K-Anonimização do Identificador)		0,31

05. No caso em estudo, não foram identificadas variáveis contextuais que impactem significativamente no risco de reidentificação, sendo o fator de ponderação definido em 1,00. Conforme proposto no processo, o Risco Mensurado de Reidentificação é o valor resultante da ponderação entre as variáveis contextuais e a métrica contextual, no exemplo 1,00*0,31 = 0,31.

06. O Risco de Reidentificação Mensurado calculado é de 0,31, enquanto o Risco de Reidentificação Aceitável é de 0,35. De tal forma, o conjunto de dados após a aplicação do conjunto de técnicas de anonimização tem um risco de reidentificação menor do que o risco aceitável.

07. De acordo com o processo proposto, é necessário acompanhar o risco mensurado de reidentificação para que ele sempre se mantenha abaixo do risco de reidentificação aceitável.

DocuSigned by:
Marcelo Takeyama
6014FFDCF2F6469...
Juridico Abecs

DocuSigned by:
Luís Vicente Magni De Chiara
90648D5D0B4C4BD...
Febraban

DocuSigned by:
Carolina Sansão Moreira Alexandrino
9AC4593ECAF84A4...
FEBRABAN

Consulta Pública ANPD – Estudo Preliminar – Anonimização e pseudonimização para proteção de dados

1 – Comentários ao item 2.2:

a) Comentário: Recomendamos que o termo "condicionante para o tratamento" constante na tabela do item 2.2 seja substituído por "prática recomendada para o tratamento".

Situações e Aplicação das técnicas na LGPD	Processo
Condicionante para o tratamento nas hipóteses do uso dos dados pessoais e dados pessoais sensíveis em pesquisas – art. 7º, inciso IV; art. 11, alínea "c" do inciso II;	Anonimização
Reversão do processo de anonimização – art. 12, *caput* e §§ 1º e 3º;	Anonimização
Tratamento de dados sensíveis – estudos e pesquisas em saúde pública – art. 13, *caput* e § 4º.	Pseudonimização
Conservação dos dados após o término do tratamento – *caput* no art. 16, incisos II e IV;	Anonimização
Direito dos titulares no art. 18, inciso IV; **compartilhamento e da portabilidade de dados** - § 6º e 7º do art. 18.	Anonimização

b) Fundamento: O uso do termo "condicionante" pode levar ao entendimento equivocado de que as hipóteses legais presentes nos arts. 7°, IV e 11, II, c apenas podem ser utilizadas se, previamente, o agente de tratamento anonimizar esses dados. Entendemos que essa interpretação não está alinhada com a intenção do legislador, nem com entendimentos apresentados pela própria ANPD.

Assim, para se evitar entendimento equivocado sobre o tema, contraditório com o próprio posicionamento pregresso da ANPD, recomendamos que o termo "condicionante para o tratamento" constante na tabela do item 2.2 seja substituído por "prática recomendada para o tratamento", refletindo de forma mais apropriada a intenção do legislador: recomendar a adoção de controle específico visando garantir a maior segurança ao titular.

2 – Comentários ao item 3.1.1 (§§27-32):

a) Comentário: Recomendamos que seja expressamente incluído no item 3.1.1 informação no seguinte sentido: "o processo de anonimização poderá ser fundamentado na mesma base legal que justificou a coleta e manutenção originária do dado, desde que a finalidade da anonimização não seja incompatível com a finalidade desta operação de tratamento original".

b) Fundamento: Os §§27-32 do Estudo Preliminar levam ao entendimento de que toda a carga regulatória aplicável habitualmente às operações de tratamento (inclusive a necessidade de fundamentação em uma base legal) seriam aplicáveis à anonimização; no entanto, por questões

FIESP – Federação das Indústrias do Estado de São Paulo
Av. Paulista, 1313 – 01311-923 / São Paulo – SP
Tel.: 11 3549.4499 – Fax: 11 3284.3611
www.fiesp.com.br

técnicas e práticas, não entendemos que esse entendimento seja adequado, sobretudo em relação à necessidade de subsunção a uma base legal do processo de anonimização analisado isoladamente.

A distinção é importante pois, interpretando de forma diversa, toda etapa de processo que envolva dados pessoais precisaria ser individualmente fundamentada em uma base legal.

Seguindo esse entendimento, a atividade de anonimização não deve ser encarada como operação de tratamento em si mesma, mas como parte integrante de uma operação de tratamento prévia (aquela que originou a coleta dos dados pelo agente de tratamento), usualmente marcando o encerramento dessa operação – nessa linha, não deve, por exemplo, ser interpretado de forma diferente da atividade de descarte de dados ou de implementação de medida de segurança que afete os dados em questão, como a criptografia.

Além disso, ainda que a atividade de anonimização não se destine a encerrar a operação de tratamento, mas a permitir que os dados, agora anonimizados, sejam utilizados em novo formato, entendemos que o processo de anonimização poderá ser tratado conforme a base legal originária, desde que seja compatível com a finalidade para a qual o dado foi originalmente coletado (e acreditamos que isso deve ser entendido como regra).

Tudo exposto, recomendamos que seja expressamente incluído no item 3.1.1 informação no seguinte sentido: "o processo de anonimização poderá ser fundamentado na mesma base legal que justificou a coleta e manutenção originária do dado, desde que a finalidade da anonimização não seja incompatível com a finalidade dessa operação de tratamento originária".

3 – Comentários ao item 3.1.1 (§§33-37):

a) Comentário: Recomendamos que, para garantia de segurança jurídica, seja expressamente incluída no item 3.1.1 informação no sentido de que "em regra, presume-se que a anonimização, é compatível com a finalidade originária do tratamento".

b) Fundamento: apesar de se reconhecer a importância da compatibilidade de todos os processos envolvendo o tratamento de dados pessoais com as finalidades originalmente informadas aos titulares, para se evitar insegurança jurídica é necessário esclarecer a compatibilidade, como regra, das operações de anonimização com as finalidades originárias, ressalvadas situações absolutamente excepcionais.

Diante disso, recomendamos que, para garantia de segurança jurídica, seja expressamente incluída no item 3.1.1 informação no sentido de que "em regra, presume-se que a anonimização, é compatível com a finalidade originária do tratamento".

4– Comentários ao item 3.1.1 (§§38-40):

a) Comentário: Recomendamos a remoção dos §§38-40 do Guia e a inclusão de informativo no

FIESP – Federação das Indústrias do Estado de São Paulo
Av. Paulista, 1313 – 01311-923 / São Paulo – SP
Tel.: 11 3549.4499 – Fax: 11 3284.3611
www.fiesp.com.br

sentido de que “a anonimização e a pseudonimização são atividades por intermédio da quais o agente de tratamento pode atender ao princípio da necessidade”.

b) Fundamento: Nos §§38-40 do Estudo Preliminar em análise, a ANPD parece indicar que o processo de anonimização necessita passar por prévia validação à luz do princípio da necessidade.

Ao nosso entender, entretanto, essa orientação deve ser eliminada, uma vez que o processo de anonimização é ferramenta que concretiza o princípio da necessidade, não fazendo sentido, por conseguinte, que de forma prévia a sua aplicação se imponha um estudo preliminar sobre a aplicação deste princípio.

Assim, entendemos que, no lugar de submeter o processo de anonimização a verificação prévia de sua compatibilidade com o princípio da necessidade – o que, em regra, se revelará não apenas processo burocrático sem real sentido, mas também como desincentivo a se seguir com a anonimização – a ANPD deve destacar o papel de anonimização e da pseudonimização na estratégia de minimização de dados. Para tanto, recomendamos a remoção dos §§38-40 do Guia e a inclusão de informativo no sentido de que “a anonimização e a pseudonimização são atividades por intermédio das quais o agente de tratamento pode atender ao princípio da necessidade”.

5 – Comentários ao item 3.1.3 (§§50-52):

a) Comentário: considerando que (i) a interpretação a ser fornecida pela ANPD em seu guia não pode se operar de forma contrária à legislação em detrimento do agente regulado; e (ii) o legislador pátrio optou por apontar “fatores objetivos” e “utilização exclusiva de meios próprios” como critérios cumulativos para a avaliação do “esforço razoável”, é necessário que o teor dos §§50-52 seja alterado, de modo que seja esclarecido que, no contexto da LGPD, a análise da eficácia da anonimização é limitada aos meios razoavelmente disponíveis ao agente de tratamento, inclusive quanto a análise dos “esforços razoáveis”, ainda que outros meios estejam disponíveis no mercado.

b) Fundamento: em seu item 3.1.3, o Estudo Preliminar fornece proposta de interpretação ao entendimento a respeito da suficiente “irreversibilidade” à luz do art. 12 da LGPD.

Nesse sentido o mencionado guia acertadamente afirma ao se avaliar a irreversibilidade, o *caput* do art. 12 requer que sejam considerados dois requisitos: (*i*) esforços razoáveis; e (*ii*) meios próprios. No entanto, ao descrever os elementos que constituem o “esforço razoável”, o Estudo Preliminar, influenciado pela regulação europeia, tratou o conceito de “esforço razoável”, como conceito que não fica restrito aos limites do agente regulado, mas observa, também, as práticas disponíveis no mercado.

Ocorre que a redação dada pelo legislador pátrio para conceituar o que considera “esforços razoáveis” não equivale ao entendimento europeu sobre o tema.

Em outras palavras: pela opção de redação do legislador pátrio, ainda que uma tecnologia apta a reidentificar o titular esteja razoavelmente disponível no mercado, caso ela não se encontre à

FIESP – Federação das Indústrias do Estado de São Paulo
Av. Paulista, 1313 – 01311-923 / São Paulo – SP
Tel.: 11 3549.4499 – Fax: 11 3284.3611
www.fiesp.com.br

disposição do agente de tratamento que praticou o processo de anonimização, não pode ser considerado "meio razoável".

Assim, considerando que (*i*) a interpretação a ser fornecida pela ANPD em seu guia não pode se operar de forma contrária à legislação em detrimento do agente regulado; e (*ii*) o legislador pátrio optou por apontar "fatores objetivos" e "utilização exclusiva de meios próprios" como critérios cumulativos para a avaliação do "esforço razoável", é necessário que o teor dos §§50-52 seja alterado, de modo que seja esclarecido que, no contexto da LGPD, a análise da eficácia da anonimização é limitada aos meios razoavelmente disponíveis ao agente de tratamento, inclusive quanto a análise dos "esforços razoáveis", ainda que outros meios estejam disponíveis no mercado.

6 – Comentários ao item 3.3 (§76):

a) Comentário: recomendamos a substituição da frase "A pseudonimização de dados pessoais significa substituir quaisquer características identificáveis dos dados por um pseudônimo, ou seja, um valor que não permite a identificação direta do titular dos dados" por "a pseudonimização de dados pessoais significa substituir, remover ou transformar quaisquer identificadores diretos dos dados".

b) Fundamento: A frase mencionada acima, conforme texto apresentada pelo guia proposto, leva ao entendimento equivocado de que a presença de identificadores indiretos em uma base de dados, por si só, leva à sua descaracterização (ou, pelo menos, dos dados vinculados a esses identificadores) como pseudonimizada. Esse entendimento não está alinhado com as melhores práticas sobre o tema e, em última instância, torna a pseudonimização impossível ou, minimamente, indesejável.

Pseudonimizar, como o próprio Guia proposto apresenta, não é retirar a característica do dado como "dado pessoal"; assim, um dado pseudonimizado precisa ser informação relacionada a uma "*pessoa física identificada* ***ou*** *identificável*".

Assim, recomendamos que a redação da primeira frase do §76 passe a ser: "A pseudonimização de dados pessoais significa substituir, remover ou transformar quaisquer identificadores diretos dos dados".

7 – Comentários ao item 3.3 (§84):

a) Comentário: Recomendamos que a frase "algumas etapas devem ser observadas" no §84, seja substituída por "é recomendável que algumas etapas sejam observadas".

b) Fundamento: A expressão "algumas etapas devem ser observadas" leva à conclusão de que a observância do procedimento apresentado pela ANPD é necessária para a execução da uma pseudonimização eficaz ou, minimamente, o desenvolvimento e implementação de metodologia eficaz de pseudonimização. Ocorre que nenhuma das conclusões parece adequada.

FIESP – Federação das Indústrias do Estado de São Paulo
Av. Paulista, 1313 – 01311-923 / São Paulo – SP
Tel.: 11 3549.4499 – Fax: 11 3284.3611
www.fiesp.com.br

Referências:

[1] Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/web-guia-anpd-tratamento-de-dados-para-fins-academicos.pdf. Acesso em 16.02.2024

[2] Disponível em: https://www.dataprotection.ie/en/individuals/data-protection-basics/definition-key-terms#:~:text=The%20term%20%E2%80%9Cprocessing%E2%80%9D%20refers%20to,involve%20automated%20or%20manual%20operations. Acesso em 16.02.2024

[3] Disponível em: https://iapp.org/news/a/does-anonymization-or-de-identification-require-consent-under-the-gdpr/. Acesso em 16.02.2024

[4] Disponível em: https://iapp.org/media/pdf/resource_center/wp216_Anonymisation-Techniques_04-2014.pdf. Acesso em 16.02.2024

[5] Disponível em: https://www.aepd.es/en/prensa-y-comunicacion/blog/anonymisation-and-pseudonymisation. Acesso em 16.02.2024

[6] Disponível em: https://iapp.org/media/pdf/resource_center/wp216_Anonymisation-Techniques_04-2014.pdf. Acesso em 16.02.2024

[7] Disponível em: https://ico.org.uk/media/about-the-ico/consultations/2619862/anonymisation-intro-and-first-chapter.pdf. Acesso em 16.02.2024

[8] Disponível em: https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190614%20Anonymisation%20and%20Pseudonymisation.pdf. Acesso em 16.02.2024

[9] Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em 16.02.2024

[10] Disponível em: https://edpb.europa.eu/sme-data-protection-guide/secure-personal-data_en#:~:text=Pseudonymisation%20is%20the%20processing%20of,to%20technical%20and%20organisational%20measures.. Acesso em 16.02.2024

[11] Disponível em: https://ico.org.uk/media/about-the-ico/consultations/4019579/chapter-3-anonymisation-guidance.pdf. Acesso em 16.02.2024

[12] Disponível em: https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190614%20Anonymisation%20and%20Pseudonymisation.pdf. Acesso em 16.02.2024

[13] Disponível em: https://ico.org.uk/media/about-the-ico/consultations/4019579/chapter-3-anonymisation-guidance.pdf. Acesso em 16.02.2024

FIESP – Federação das Indústrias do Estado de São Paulo
Av. Paulista, 1313 – 01311-923 / São Paulo – SP
Tel.: 11 3549.4499 – Fax: 11 3284.3611
www.fiesp.com.br

CONSULTA À SOCIEDADE - ANPD

ESTUDO TÉCNICO SOBRE A ANONIMIZAÇÃO DE DADOS NA LGPD

I. Apresentações

A Telefônica Brasil S.A, detentora da marca "Vivo", oferece aos seus clientes um completo portfólio de produtos, incluindo serviços de voz (fixos e móveis), dados móveis, ultra banda larga, TV por assinatura, tecnologia da informação e serviços digitais. Nosso propósito é "Digitalizar para aproximar", o que reforça nosso compromisso de levar conexão de qualidade e inclusão digital para pessoas e empresas em todo o território nacional, pois acreditamos que a conectividade é a porta de entrada para o mundo digital e pode gerar muitas oportunidades para todos.

A Vivo se preocupa com a segurança no tratamento dos dados pessoais de seus clientes e se pauta em três pilares fundamentais: a confidencialidade, a integridade e a disponibilidade das informações que gerimos. Como parte do nosso compromisso e em conformidade com a legislação aplicável, adotamos medidas de segurança robustas com o objetivo de evitar incidentes, utilizando recursos para identificação e correção de vulnerabilidades que possam colocar em risco a privacidade de nossos clientes, colaboradores e parceiros.

Nosso compromisso com a proteção e privacidade de dados existe mesmo antes da publicação da Lei e se intensificou a partir de 2018 quando a Vivo iniciou sua adequação às regras e obrigações impostas pela LGPD por meio de um grupo de trabalho especializado, multidisciplinar e capacitado.

O presente documento apresenta considerações da Vivo, sob a assinatura do seu Escritório de Privacidade, sobre o Estudo Técnico de anonimização e pseudonimização, elaborado pela Autoridade Nacional de Proteção de Dados (ANPD).

Congratulamos o Conselho Diretor da ANPD pela promoção do diálogo diante de temas importantes e de fundamental atenção para que todas as partes interessadas possam apresentar suas considerações visando contribuir para as premissas estabelecidas pela LGPD, proteger os direitos fundamentais de liberdade e privacidade, garantir o livre desenvolvimento da personalidade da pessoa natural e fomentar inovações, novas tecnologias e usos associados ao tratamento de dados pessoais no Brasil.

II. Introdução

A Lei Geral de Proteção de Dados menciona conceitos importantes. Entre eles, podemos citar o conceito "core" da legislação, a definição de dados pessoais.

Em seu Artigo 5º, I, a definição de dado pessoal é: "*I - dado pessoal: informação relacionada a pessoa natural* ***identificada*** *ou* ***identificável****".* – Grifamos

Assim, para que seja aplicada a LGPD, deverá existir o tratamento de dados pessoais, em consonância com a própria definição existente na Lei.

Adiante, ainda tratando-se da parte conceitual, a LGPD menciona, também no Art. 5º, a definição de anonimização dos dados pessoais:

> XI - *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****."* – grifamos e sublinhamos

O objeto do presente Estudo, conforme dispõe o próprio material disponibilizado, *visa compreender os fundamentos jurídico-normativos do processo de anonimização de dados na sistemática da LGPD no ordenamento jurídico brasileiro*.

Assim, é de extrema importância destacarmos os conceitos elencados na legislação, objetivando uma maior clareza e segurança jurídica na aplicação técnica e normativa sobre anonimização no tratamento dos dados pessoais.

III. Entendimentos e contribuições da Vivo referente ao Estudo Técnico sobre a anonimização de dados na LGPD

Em continuação às apresentações e da introdução sobre o tema, a Vivo apresenta seus entendimentos e contribuições ao Estudo Técnico promovido pela ANPD acerca da anonimização de dados na LGPD , seguindo o que se encontra a seguir:

1- DA NECESSIDADE DE OBSERVAÇÃO QUANTO AOS CONCEITOS LEGAIS DE DADO PESSOAL E ANONIMIZAÇÃO, PREVISTOS NA LGPD

Como a própria ANPD relata, o estudo técnico em questão *visa compreender os fundamentos jurídico-normativos do processo de anonimização de dados na sistemática da LGPD no ordenamento jurídico brasileiro*.

Em que pese o estudo técnico ser direcionado para compreensão dos fundamentos jurídico-normativos do processo de anonimização na sistemática da LGPD, é imprescindível que alguns pontos sejam devidamente destacados.

Na página 9 do referido Estudo Técnico, menciona sobre a necessidade de cumprimento aos princípios e fundamentos da LGPD, por entender a existência de tratamento de dados pessoais anterior ao processo de anonimização. Não obstante, no mesmo parágrafo, há menção sobre a necessidade de **compatibilidade de finalidade** nos casos em que houver o "tratamento posterior" ou "uso secundário" **dos dados anonimizados**.

Ocorre que, conforme elencado no tópico introdutório acima, a LGPD traz, em seu artigo 5º, a definição do que é dado pessoal e o qual o conceito de anonimização:

"I - dado pessoal: informação relacionada a pessoa natural ***identificada*** *ou* ***identificável****"* - grifamos

> XI - *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****."* – grifamos e sublinhamos

Nesse sentido, uma vez que o dado pessoal é anonimizado, ele perde a possibilidade de associação direta ou indireta do indivíduo, não sendo, portanto, considerado um dado pessoal e, assim, não sendo aplicada a Lei Geral de Proteção de Dados.

Dessa forma, não há o que se falar em aplicabilidade de fundamentos e princípios constantes na LGPD após a anonimização dos dados pessoais. Observa-se que não se trata de uma "boa prática" a ser cumprida pelos agentes de tratamento, mas sim de uma inaplicabilidade legal ao caso concreto. Se não há existência de dados pessoais, não há o que se falar em observação à LGPD.

É importante destacar que tal definição mostra-se contraditória com o item 54 da minuta do guia de anonimização, no qual destaca e reforça o seguinte:

> *Item 54 - Convém ressaltar que os dados que tenham sido tornados irreversivelmente anonimizados* ***deixam de ser considerados "dados pessoais"*** *e o processamento desses dados* ***não exige conformidade com a legislação de proteção de dados****.* – grifamos

Assim, observa-se que há contradição quanto ao disposto no Estudo Técnico, no material disponibilizado pela própria ANPD nomeado como "minuta do guia de anonimização" e nos conceitos existentes na Lei Geral de Proteção de Dados.

2- DA POSSIBILIDADE DE REVERÇÃO DO PROCESSO DE ANONIMIZAÇÃO. UTILIZAÇÃO EXCLUSIVA DE MEIOS PRÓPRIOS.

Nas páginas 13 e 14 do Estudo Técnico, menciona que "meios próprios" constante no Art. 12 da LGPD, de acordo com o considerando n. 26 da revogada diretiva europeia e do vigente Regulamento Geral de Proteção de Dados da UE, são tratados como meios suscetíveis de serem utilizados para (re)identificação de titular de dados aqueles adotados **"seja pelo responsável pelo tratamento, seja por qualquer outra pessoa".**

Ocorre que, conforme constante na própria minuta sobre o presente tema, no item 52, temos o seguinte:

> *Diferentemente da noção de "esforços razoáveis", o conceito de meios próprios* ***tem conteúdo mais delimitado, podendo-se afirmar que são*** *meios próprios as habilidades, os dados,* ***instrumentos e técnicas disponíveis ao próprio agente de tratamento responsável pela anonimização****. Sendo assim, importa ressaltar que, a partir do texto normativo do art. 12, caput, da LGPD, compreende-se que a avaliação da possibilidade de reidentificação de dados e a reversão do processo de anonimização* ***devem ter em consideração não apenas o uso de meios próprios do agente de tratamento responsável pela anonimização, mas também a atuação de outras pessoas ou entidades*** *que, com meios e esforços razoáveis, podem reidentificar conjunto de dados anonimizados.*

No trecho acima, temos a contradição entre o que, de fato, será considerado "uso de meios próprios".

Ainda, que a Lei Geral de Proteção de Dados tenha sido inspirada no ordenamento jurídico Europeu (GDPR), é importante destacar que não é uma cópia da legislação europeia, devendo a interpretação ser realizada com a maior proximidade do que dispõe no próprio texto da Lei.

A interpretação que mais se aproxima da realidade trazida pelo legislador na LGPD é a de que o uso de meios próprios será considerado os utilizados pelo próprio agente de tratamento responsável pela anonimização.

Essa definição é extremamente importante para que não ocorra qualquer responsabilização do agente de tratamento que realizou a transferência dessas informações anonimizadas para o terceiro, sem que houvesse uma observação ao processo de governança em privacidade e proteção de dados pessoais, uma vez que, teoricamente, não há o que se falar em aplicabilidade da Lei Geral

de Proteção de Dados aos dados pessoais anonimizados, no qual deixam de ser dados pessoais e passam a integrar apenas à cadeia de dados.

NOTA TÉCNICA

Consulta pública sobre anonimização e pseudonimização para proteção de dados

Brasília, 28 de fevereiro de 2024.

Ref.: Contribuição do IAB Brasil para a Consulta à Sociedade sobre o Estudo Preliminar relativo à anonimização e pseudonimização para proteção de dados

📕 INTRODUÇÃO

O IAB Brasil[1] gostaria de contribuir para a consulta à Sociedade da ANPD sobre anonimização e pseudonimização para proteção de dados[2]. Na visão da entidade, há pontos que devem ser levados em consideração, de forma a contribuir para o aperfeiçoamento do Estudo Preliminar: A minuta do guia de anonimização e pseudonimização para proteção de dados pessoais afirma que o dado anonimizado é o resultado de um processo de anonimização feito por um agente de tratamento que, para retirar os identificadores diretos e indiretos, teve acesso aos dados pessoais. O documento assinala, ainda, que, no atual estado da arte, não há como excluir o risco de reidentificação, independentemente da técnica utilizada para a anonimização, motivo pelo qual caberia ao agente de tratamento, gerenciar o risco de reidentificação e a utilidade dos dados anonimizados num processo de anonimização baseada em risco. Nesse processo, o agente de tratamento deveria mensurar o RRM (Risco de Reidentificação Censurado) de acordo com a realidade de cada agente de tratamento (a Métrica Contextual).

📕 INTRODUÇÃO E COMENTÁRIOS GERAIS

Seria importante, porém, deixar expressa a possibilidade de o processo de anonimização ser considerado eficaz ainda que identificadores indiretos não sejam completamente removidos,

[1] O IAB Brasil é uma entidade sem fins lucrativos que tem como principal missão o desenvolvimento da mídia interativa no Brasil, contando atualmente com mais de 265 associados, entre anunciantes, veículos produtores de conteúdo, empresas de tecnologia, agências e desenvolvedores, líderes em seu segmento no país. De forma exemplificativa, o IAB Brasil busca desenvolver a publicidade online no Brasil através das seguintes ações: (i) incentivo às boas práticas para o planejamento, criação, compra, venda, veiculação e mensuração de mensagens comerciais; (ii) desenvolvimento do intercâmbio de experiências e conhecimentos técnicos de seus associados; (iii) promoção e divulgação de pesquisas e estudos que comprovem a eficiência da mídia interativa; e (iv) promoção da identificação de oportunidades de posicionamento da mídia interativa através de linguagem publicitária, para atrair o interesse de anunciantes e profissionais da mídia tradicional. Mais informações sobre o IAB Brasil estão disponíveis no site https://iabbrasil.com.br/sobre-iab/ .

prejudicados ou tornados inúteis dentro de um conjunto de dados, sempre que a probabilidade de reidentificação dos titulares permaneça em nível suficientemente remoto. Por exemplo, certos identificadores indiretos, como gênero, estado e idade, normalmente podem ser utilizados dentro de um conjunto de dados anonimizados sem que haja possibilidade de identificação de seus titulares.

Nesse contexto, a minuta do guia afirma que os seguintes elementos devem ser levados em consideração durante a avaliação dos riscos de reidentificação sobre dados anonimizados: a distinção (singling-out), a possibilidade de ligação (linkability) e a inferência (inference). Ainda que tal posicionamento se mostre alinhado à interpretração europeia sobre o tema (inclusive com referências expressas do Information Commissioner Office), o IAB Brasil pondera que a mera associação de dados a respeito de um mesmo indivíduo desconhecido, ou a extração de presunções sobre grupos de pessoas não identificadas ou identificáveis, é incapaz de prejudicar ou tornar ineficaz o processo de anonimização de dados. Em caso de entendimento diverso por parte da Autoridade, o uso de dados anonimizados se mostraria substancialmente inútil em boa parte dos casos de uso mais relevantes ao tema, tornando, eventualmente, a regulação totalmente avessa à realidade.

A LGPD e a própria minuta do guia estabelecem que os dados anonimizados não são considerados dados pessoais, exceto quando o processo de anonimização for revertido *"usando exclusivamente meios próprios ou quando, com esforços razoáveis, puder ser revertido"*.

Neste contexto, destaca-se que existem inúmeros modelos de negócios em que o serviço prestado utiliza exclusivamente dados anonimizados fornecidos pelo contratante. Em outras palavras, o prestador de serviços jamais teve (ou terá) acesso aos identificadores diretos ou indiretos ou aos dados pessoais.

Nesse cenário, é importante o esclarecimento da Autoridade no sentido de que esses prestadores de serviços, seja porque não participaram do processo de anonimização ou porque não tratam dados pessoais, não são responsáveis pelo gerenciamento do risco de reidentificação, cabendo essa responsabilidade apenas ao agente de tratamento que realizou o processo de anonimização.

Adicionalmente, é importante o esclarecimento da Autoridade no sentido de que a Métrica Contextual deverá ser mensurada conforme a realidade do agente de tratamento que efetivamente realizou o processo de anonimização, e não a realidade dos prestadores de serviços que somente trabalham com os dados anonimizados.

Esse ponto é crucial, já que o conceito de pseudonimização adotado pela LGPD consiste no tratamento de dados não-identificados, mas que podem ser reidentificados **pelo mesmo controlador a qualquer tempo**, como destaca a lei em seu artigo 13, parágrafo 4º. Vale também recordar que a reversibilidade é a principal diferença entre a pseudonimização e anonimização: se é possível ao agente de tratamento reverter o processo, os dados serão considerados pseudonimizados e sujeitos à aplicação da LGPD.

Ou seja: no contexto do compartilhamento de dados pseudonimizados com terceiros, a capacidade de o próprio controlador realizar a reidentificação significa que os dados serão considerados

pseudonimizados **apenas em relação a ele.** Os dados serão considerados **anonimizados** pelos terceiros que recebem esses dados sempre que esses terceiros não tiverem acesso a qualquer informação do controlador que permitiria a reidentificação dos dados, como ocorre na esmagadora maioria dos casos.

Em suma, como regra geral os dados considerados pseudonimizados pelo controlador serão considerados anonimizados pelo terceiro receptor, salvo se esse terceiro consiga desfazer a pseudonimização ou reidentificar o dado - o que normalmente não será o caso.

Por essas razões, de forma a garantir segurança jurídica aos agentes de tratamento, o IAB Brasil entende ser necessário que essa Autoridade esclareça no guia a distinção entre os métodos de pseudonimização e anonimização no contexto do compartilhamento de informações e de bases de dados entre agentes de tratamento, já que o terceiro receptor que não possui acesso ao "segredo" da anonimização (seja qual for seu método) estará recebendo dados anonimizados, que não são considerados dados pessoais e, consequentemente, não se sujeitam à aplicação da LGPD. Deste modo, estes terceiros também não serão responsáveis pelo gerenciamento do risco de reidentificação, cabendo essa responsabilidade apenas ao agente de tratamento que realizou o processo de anonimização.

Ainda que seja possível que o surgimento de novas tecnologias ou a disponibilização futura de novos conjuntos de dados venham a contribuir para a elevação do risco de reversão de processos de anonimização, esse risco não pode ser considerado a partir de situações meramente hipotéticas, improváveis ou de difícil ocorrência. O que se deve esperar como resultado do processo de anonimização é uma redução da probabilidade de identificação dos titulares a nível suficientemente remoto, sendo inexigível o alcance de um risco zero de reidentificação.

Além disso, o IAB Brasil entende que uma interpretação detalhada sobre os termos "meios próprios" e "esforços razoáveis" deve fazer parte do futuro guia. A interpretação do conceito de "meios próprios" proposta preliminarmente pela Autoridade parece deixar, equivocadamente, de reconhecer a possibilidade de um mesmo conjunto de dados possuir naturezas diferentes para organizações distintas. Como destacado anteriormente, é possível que um mesmo conjunto de dados submetidos a um processo de descaracterização de identidade por uma organização A seja considerado como um conjunto de dados pseudonimizados para essa organização A e um conjunto de dados anonimizados para uma organização B, bastando que a possibilidade de reidentificação da identidade dos titulares não seja possível a essa empresa B mediante o uso dos seus próprios recursos, mas que somente a organização A tenha condições de reverter o processo utilizando o seu próprio ferramental ou base de dados auxiliar. Essa interpretação independe do fato de organizações A e B serem, ou não, pertencentes a um mesmo grupo econômico. Tal entendimento está alinhado ao posicionamento do Information Commissioner Office (ICO), no documento *"Introduction to Anonymisation - Draft anonymisation, pseudonymisation and privacy enhancing technologies guidance"*, referência global no tema anonimização de dados.

Reforçando essa lógica, ao abordar a pseudonimização de dados, a minuta do guia relaciona algumas técnicas consideradas pela Autoridade como compatíveis com a LGPD, como a substituição de dados,

a ofuscação de dados, a tokenização, a cifração, o mascaramento e o *salting*. No entanto, embora tais medidas sejam típicas do emprego da técnica de pseudonimização, é preciso ter em consideração que o resultado gerado pela descaracterização de identidade por meio da aplicação de qualquer delas pode culminar em um conjunto de dados anonimizados para uma organização terceira que não seja capaz de, mediante o emprego de esforços razoáveis e por meios próprios, reidentificar os titulares ou reestabelecer os dados em sua versão original. Dessa forma, entende-se que as técnicas relacionadas pela Autoridade não representam necessariamente técnicas exclusivas de pseudonimização de dados, podendo também funcionar como técnicas para anonimização de dados em relação a terceiros.

Outros pontos do documento merecem atenção. A minuta do guia sugere que a avaliação de compatibilidade da anonimização de dados leve em consideração *"as expectativas legítimas dos titulares e os possíveis impactos do tratamento posterior sobre seus direitos"*. No entanto, a consideração das expectativas legítimas dos titulares é tema relacionado ao uso do legítimo interesse como base legal de tratamento. A LGPD não sugere que "expectativas legítimas" dos titulares sejam consideradas como um fator relevante para legitimar o processo de anonimização de dados, inclusive porque o processo de anonimização pode ser complexo e pouco compreensível à pessoa média, sendo irrazoável pressupor que alguém, sem razão aparente, teria uma efetiva expectativa de que seus dados pudessem ser submetidos a um processo de anonimização em determinado momento ou contexto.

Além disso, a minuta do guia afirma que *"a pertinência da adoção do processo de anonimização decorre de um juízo de necessidade"* pelo agente de tratamento, que deve ser realizado *"à luz da(s) finalidade(s) especificada(s) para o tratamento de dados na situação concreta"*. No entanto, a aplicação do processo de anonimização não decorre, exclusivamente, de uma necessidade constatada, podendo derivar de uma conveniência ou oportunidade identificada pelo agente. A anonimização de dados pode ser tida como uma medida relevante para a realização de atividades econômicas de maneira mais compatível com a segurança e com a privacidade, ainda que existam alternativas que permitam ao agente alcançar as mesmas finalidades sem anonimizar os dados. Nesse caso, o agente de tratamento decide a respeito da anonimização de dados à luz de um juízo de relevância e conveniência, e não de mera necessidade. Dessa forma, entende-se que melhor atuaria a Autoridade se consignasse expressamente o entendimento de que a anonimização pode decorrer da necessidade, da relevância ou da conveniência.

A minuta do guia apresenta fluxo para pseudonimização ("Metodologia Eficaz de Pseudonimização") com 12 etapas - entre as quais a elaboração de uma avaliação de impacto à proteção de dados pessoais (etapa 11). No entanto, esse ponto merece ser melhor esclarecido, para que não se crie nos agentes de tratamento uma falsa percepção de que todas as atividades envolvendo pseudonimização de dados demandariam a condução de um Relatório de Impacto à Proteção de Dados Pessoais de maneira indiscriminada, posto que a atividade de pseudonimização, por si só, é incapaz de gerar alto risco às liberdades e aos direitos dos titulares (requisito essencial para a necessidade de elaboração de um RIPD). Referido posicionamento, de maneira mais objetiva, evitará que os agentes de tratamento sofram com ônus operacionais e financeiros na condução de RIPDs desnecessários.

Por fim, entre as etapas inseridas nessa "Metodologia Eficaz de Pseudonimização", está a comunicação aos titulares. A minuta sugere que o agente de tratamento deve estar *"preparado para informar de forma transparente e acessível aos titulares sobre a pseudonimização"*. No entanto, a LGPD não prevê a comunicação com os titulares como um pressuposto essencial à aplicação das técnicas de pseudonimização de dados. O dever de comunicação com os titulares (princípio da transparência) deve ser regularmente aplicado a todas as atividades de tratamento que envolvam dados pessoais, sem qualquer tipo de obrigação incremental nas atividades envolvendo a pseudonimização de dados. Caso mantido esse entendimento, o IAB Brasil sugere que sejam apresentadas diretrezes concretas sobre o contexto no qual essa comunicação se mostraria exigível, bem como seu conteúdo e escopo esperados. Acredita-se que questões pura ou majoritariamente técnicas, como a modalidade de pseudonimização aplicada pelo agente de tratamento, não devam ser reveladas, sob pena de potencialização dos riscos de tentativas externas de reversão da técnica empregada.

Permanecemos à inteira disposição para colaborar em tudo que esteja ao nosso alcance.

_____

CRISTIANE CAMARGO

(CEO do IAB Brasil)

A Federação do Comércio de Bens, Serviços e Turismo do Estado de São Paulo ("FecomercioSP"), vem apresentar os seus comentários à minuta de Estudo Preliminar de Anonimização e Pseudonimização para a proteção de dados pessoais apresentada pela Autoridade Nacional de Proteção de Dados ("ANPD") para consulta à sociedade:

1 – Comentários ao item 2.2:

a) Comentário: Recomendamos que o termo "condicionante para o tratamento" constante na tabela do item 2.2 seja substituído por "prática recomendada para o tratamento".

Situações e Aplicação das técnicas na LGPD	Processo
Condicionante para o tratamento nas hipóteses do uso dos dados pessoais e dados pessoais sensíveis em pesquisas – art. 7º, inciso IV; art. 11, alínea "c" do inciso II;	Anonimização
Reversão do processo de anonimização – art. 12, *caput* e §§ 1º e 3º;	Anonimização
Tratamento de dados sensíveis – estudos e pesquisas em saúde pública – art. 13, *caput* e § 4º.	Pseudonimização
Conservação dos dados após o término do tratamento – *caput* no art. 16, incisos II e IV;	Anonimização
Direito dos titulares no art. 18, inciso IV; **compartilhamento e da portabilidade de dados** - § 6º e 7º do art. 18.	Anonimização

b) Fundamento: O uso do termo "condicionante" pode levar ao entendimento equivocado de que as hipóteses legais presentes nos arts. 7º, IV e 11, II, c apenas podem ser utilizadas se, previamente, o agente de tratamento anonimizar esses dados. Entendemos que essa interpretação não está alinhada com a intenção do legislador, nem com entendimentos apresentados pela própria ANPD.

Em relação a intenção legislativa, destacamos que em ambas as mencionadas bases legais o legislador se utilizou da expressão "garantida, sempre que possível, a anonimização dos dados pessoais".

O termo, "sempre que possível", por si só, é indicativo de que a anonimização não é condicionante para a fundamentação da operação de tratamento em quaisquer das mencionadas hipóteses legais, mas recomendação, vez que nas hipóteses em que a anonimização não se faça possível (seja porque inviável de ser executada na prática pela organização,

seja porque na situação concreta não se faça adequada), a base legal ainda assim poderá ser empregada.

Concluir de forma diversa implicaria em admitir verdadeira contradição lógica por parte do legislador, visto que, conforme expressa a própria LGPD, dados anonimizados não são considerados dados pessoais (art. 12, *caput*), pelo que inaplicáveis a eles o regramento relativo ao tratamento de dados pessoais e, portanto, desnecessária a fundamentação em uma base legal. Em outras palavras: as hipóteses legais em análise restariam desprovidas de qualquer valor, vez que para a sua aplicação seria necessário anonimizar os dados, mas uma vez anonimizados o uso dessas hipóteses legais se faria dispensável.

A própria ANPD, em seu Guia Orientativo sobre o Tratamento de Dados Pessoais para Fins Acadêmicos e para a Realização de Estudos e Pesquisas[1] optou por expressamente esclarecer a ausência de condicionalidade entre a aplicação da anonimização e o uso das bases legais em análise:

> "*Em conjunto, esses dispositivos legais indicam que a anonimização ou a pseudonimização de dados pessoais não foram instituídas pela LGPD como medidas de segurança impositivas, isto é, que devem ser adotadas em todo e qualquer caso de estudos e pesquisas.*
> *Da mesma forma, a LGPD não estabeleceu a anonimização ou a pseudonimização como condição técnica para a divulgação pública ou para o compartilhamento de dados pessoais para fins de realização de estudos e pesquisas, devendo-se reconhecer, inclusive, que, em alguns casos, a identificação dos titulares pode ser imprescindível para os objetivos da pesquisa*".

Assim, para se evitar entendimento equivocado sobre o tema, contraditório com o próprio posicionamento pregresso da ANPD, recomendamos que o termo "condicionante para o tratamento" constante na tabela do item 2.2 seja substituído por "prática recomendada para o tratamento", refletindo de forma mais apropriada a intenção do legislador: recomendar a adoção de controle específico visando garantir a maior segurança ao titular.

2 – Comentários ao item 3.1.1 (§§27-32):

a) Comentário: Recomendamos que seja expressamente incluído no item 3.1.1 informação no seguinte sentido: "o processo de anonimização poderá ser fundamentado na mesma base legal que justificou a coleta e manutenção originária do dado, desde que a finalidade da anonimização não seja incompatível com a finalidade desta operação de tratamento original".

b) Fundamento: Os §§27-32 do Estudo Preliminar levam ao entendimento de que toda a carga regulatória aplicável habitualmente às operações de tratamento (inclusive a necessidade de fundamentação em uma base legal) seriam aplicáveis à anonimização; no entanto, por questões técnicas e práticas, não entendemos que esse entendimento seja adequado, sobretudo em relação à necessidade de subsunção a uma base legal do processo de anonimização analisado isoladamente.

Em se tratando de aspectos técnico-jurídicos, antes de seguir com a análise específica sobre o processo de anonimização, é necessário esclarecer o que se deve entender por "tratamento de dados": apesar de (*i*) o legislador apresentar rol de atividades exemplificativas isoladas (ex. coleta, produção, utilização...) para descrever o significado de "tratamento de dados"; e (*ii*) essas ações, se executadas isoladamente, serem enquadradas como tratamento de dados, quando as atividades são partes integrantes de processo maior, ele é que deve ser visto como o "tratamento de dados", não as atividades isoladamente. Nesse sentido segue a Autoridade de Dados da Irlanda [2]:

> "*The term "processing" refers to any operation or set of operations performed on personal data. Processing includes storing, collecting, retrieving, using, combining, erasing and destroying personal data, and can involve automated or manual operations*".

A distinção é importante pois, interpretando de forma diversa, toda etapa de processo que envolva dados pessoais precisaria ser individualmente fundamentada em uma base legal.

Essa necessidade, além de gerar diversos reflexos indesejáveis ao ecossistema de proteção de dados (por exemplo, implicaria em afirmar que cada atividade isolada precisaria ser individualmente registrada (art. 37, da LGPD), o que tornaria a manutenção do registro de operações de tratamento inexequível para a ampla maioria das organizações), pode tornar os processos organizacionais em si impraticáveis.

Seguindo esse entendimento, a atividade de anonimização não deve ser encarada como operação de tratamento em si mesma, mas como parte integrante de uma operação de tratamento prévia (aquela que originou a coleta dos dados pelo agente de tratamento), usualmente marcando o encerramento dessa operação – nessa linha, não deve, por exemplo, ser interpretado de forma diferente da atividade de descarte de dados ou de implementação de medida de segurança que afete os dados em questão, como a criptografia.

Esse é o entendimento do legislador pátrio ao apontar a anonimização de dados como uma alternativa à sua eliminação, nos termos do art. 16, IV, da LGPD.

Além disso, ainda que a atividade de anonimização não se destine a encerrar a operação de tratamento, mas a permitir que os dados, agora anonimizados, sejam utilizados em novo formato, entendemos que o processo de anonimização poderá ser tratado conforme a base legal originária, desde que seja compatível com a finalidade para a qual o dado foi originalmente coletado (e acreditamos que isso deve ser entendido como regra).

Em primeiro lugar, do ponto de vista técnico jurídico, essa é a interpretação teleológica mais adequada ao art. 9º, §2º, da LGPD, que embora se refira ao consentimento, é razoavelmente adequada a qualquer outra base legal: do mesmo modo que a necessidade de oportunizar a revogação do consentimento apenas é requerida se a finalidade for incompatível com a do consentimento originário, a necessidade de nova fundamentação da operação de tratamento também apenas deve ser necessária se a nova finalidade for incompatível. Nesse sentido, El Emam e Hintze, em artigo escrito para a IAPP[3]:

> *"In other words, the processing of personal data in order to fully anonymize it is "compatible with the purpose for which the personal data are initially collected" and therefore does not require an additional legal basis, such as consent, specifically for the act of anonymizing".*

Ainda, a conclusão em questão parece ser lógica e necessária do ponto de vista prático: se a operação de anonimização precisa ser fundamentada em nova base legal (em grande parte dos casos, sobretudo com o envolvimento de dados pessoais sensíveis, a base aplicável seria o consentimento), os agentes de tratamento serão desincentivados a adotar o processo de anonimização, vez que representará custo significativo, sem

que nenhum benefício real advenha para o agente de tratamento em questão, o que, por sua vez, acresce significativamente os riscos aos titulares.

Explicamos: digamos que empresa proprietária de uma rede de farmácias deseja utilizar sua base de dados para, com base no histórico de compras de seus clientes (que, naturalmente, envolverá dados pessoais sensíveis), desenvolver sistema de inteligência artificial para prever a demanda por reabastecimento de suas lojas. Entendemos que há dois "cenários" possíveis:

- Caso seja possível anonimizar os dados a serem utilizados sem a necessidade de fundamentar isso em base legal, ela muito provavelmente será incentivada a fazê-lo, vez que obter o consentimento individual dos titulares será tarefa complexa. Nesse cenário, ambos, empresa e titulares são beneficiados, a primeira executando a atividade desejada, os demais tendo seus dados resguardados.

- Caso não seja possível anonimizar os dados sem sua fundamentação isolada em uma base legal, a empresa, para não desistir do projeto, terá de investir recursos na coleta e no gerenciamento do consentimento dos titulares. Nessa hipótese, parece pouco crível que a empresa não opte por simplesmente buscar o consentimento para o desenvolvimento do sistema em si, ao invés da anonimização, vez que anonimizar os dados representariam um custo para o projeto sem, ao menos no futuro previsível, nenhum retorno concreto para a organização. Neste cenário, ambos, empresa e titulares são prejudicados, a primeira despendendo recursos que poderiam ter sido mais bem despendidos no processo de anonimização (que garantiria maior segurança dos dados sob a sua responsabilidade), os demais deixando de ter seus dados mais rigidamente resguardados.

Tudo exposto, recomendamos que seja expressamente incluído no item 3.1.1 informação no seguinte sentido: "o processo de anonimização poderá ser fundamentado na mesma base legal que justificou a coleta e manutenção originária do dado, desde que a finalidade da anonimização não seja incompatível com a finalidade dessa operação de tratamento originária".

3 – Comentários ao item 3.1.1 (§§33-37):

a) Comentário: Recomendamos que, para garantia de segurança jurídica, seja expressamente incluída no item 3.1.1 informação no sentido de que "em regra, presume-se que a anonimização, é compatível com a finalidade originária do tratamento".

b) Fundamento: apesar de se reconhecer a importância da compatibilidade de todos os processos envolvendo o tratamento de dados pessoais com as finalidades originalmente informadas aos titulares, para se evitar insegurança jurídica é necessário esclarecer a compatibilidade, como regra, das operações de anonimização com as finalidades originárias, ressalvadas situações absolutamente excepcionais.

Afirmamos isso considerando que: (*i*) a anonimização é processo que, em regra, objetiva (ou, no mínimo, tem como efeito necessário) garantir maior segurança aos titulares de dados, pois reduz a possibilidade de sua identificação e, consequentemente, destes serem afetados por eventuais incidentes ou irregularidades no tratamento; e (*ii*) a anonimização é prática necessária para se atender aos princípio da necessidade em seu aspecto temporal – isto é, não reter dados pessoais em formato identificável para além do tempo necessário.

Esse, aliás, aparenta ser o posicionamento pacífico das Autoridades de Dados Europeias, como se retira do posicionamento do *European Data Protection Board* (a época, Article 29 *Working Party*) em seu guia sobre o tema [4]:

> *"On the other hand, the provisions contained in Article 6(1) e) of the Directive 95/46/EC (but also in Articles 6(1) and 9(1) of the e-Privacy Directive) ought to be pointed out as they demonstrate the need to keep personal data "in a form which permits identification" for no longer than is necessary for the purposes of the collection or further processing. In itself, this provision makes a strong point that personal data should, at least, be anonymised "by default" (subject to different legal requirements, such as those mentioned in the e-Privacy Directive regarding traffic data). If the data controller wishes to retain such personal data once the purposes of the original or further processing have been achieved, anonymisation techniques should be used so as to irreversibly prevent identification. Accordingly, the Working Party considers that anonymisation as an instance of further processing of personal data can be considered to be compatible with the original purposes of the processing but only on condition the anonymisation process is such as*

> *to reliably produce anonymised information in the sense described in this paper"*

Na mesma linha, e com base na opinião acima, a Autoridade de Dados da Espanha[5]:

> " *The processing activity that produces anonymised data is a processing of personal data, which can be considered to be compatible with the original purposes of processing from which the data are obtained*"

Diante disso, recomendamos que, para garantia de segurança jurídica, seja expressamente incluída no item 3.1.1 informação no sentido de que "em regra, presume-se que a anonimização, é compatível com a finalidade originária do tratamento".

4— Comentários ao item 3.1.1 (§§38-40):

a) Comentário: Recomendamos a remoção dos §§38-40 do Guia e a inclusão de informativo no sentido de que "a anonimização e a pseudonimização são atividades por intermédio da quais o agente de tratamento pode atender ao princípio da necessidade".

b) Fundamento: Nos §§38-40 do Estudo Preliminar em análise, a ANPD parece indicar que o processo de anonimização necessita passar por prévia validação à luz do princípio da necessidade.

Ao nosso entender, entretanto, essa orientação deve ser eliminada, uma vez que o processo de anonimização é ferramenta que concretiza o princípio da necessidade, não fazendo sentido, por conseguinte, que de forma prévia a sua aplicação se imponha um estudo preliminar sobre a aplicação deste princípio.

Com efeito, como bem pontua o *European Data Protection Board*, no posicionamento acima exposto, a anonimização "por *default*" nada mais é do que o atendimento do dever de não reter os dados pessoais para além do tempo estritamente necessário[6].

Além disso, se tratando, o processo de anonimização, de uma operação voltada à minimização de dados, seja de forma estratégica, seja como consequência necessária do processo em si, este naturalmente atenderá ao princípio da necessidade, em relação ao qual a minimização de dados é

corolário, de modo que referida "avaliação preliminar da necessidade" se converterá em mera formalidade.

Nesse sentido, a Autoridade de Dados do Reino Unido destaca o papel da anonimização em apoiar o atendimento do princípio da "minimização de dados"[7]:

> "*Anonymisation limits your data protection risks, and can enable you to make information available to other organisations or to the public. It also supports the principle of data minimisation. If you process personal data, you have to comply with the data protection principles and be able to demonstrate how you do so. The principles regulate the disclosure of personal data and establish a framework through which you can do this fairly, lawfully and transparently*".

Em igual sentido, a Autoridade de Dados da Irlanda pontua a possibilidade de utilização da anonimização de dados como parte da estratégia de *privacy by design* ou de minimização de dados, mesmo quando a anonimização não é efetiva [8]:

> "*In some cases, it is not possible to effectively anonymise data, either because of the nature or context of the data, or because of the use for which the data is collected and retained. Even in these circumstances, organisations might want to use anonymisation or pseudononymisation techniques:– 1. As part of a "privacy by design" strategy to provide improved protection for data subjects 2. As part of a risk minimisation strategy when sharing data with data processers or other data controllers. 3. To avoid inadvertent data breaches occurring when your staff is accessing personal data. 4. As part of a "data minimisation" strategy aimed at minimising the risks of a data breach for data subjects*".

Assim, entendemos que, no lugar de submeter o processo de anonimização a verificação prévia de sua compatibilidade com o princípio

da necessidade — o que, em regra, se revelará não apenas processo burocrático sem real sentido, mas também como desincentivo a se seguir com a anonimização — a ANPD deve destacar o papel de anonimização e da pseudonimização na estratégia de minimização de dados. Para tanto, recomendamos a remoção dos §§38-40 do Guia e a inclusão de informativo no sentido de que "a anonimização e a pseudonimização são atividades por intermédio das quais o agente de tratamento pode atender ao princípio da necessidade".

5— Comentários ao item 3.1.3 (§§50-52):

a) Comentário: considerando que (i) a interpretação a ser fornecida pela ANPD em seu guia não pode se operar de forma contrária à legislação em detrimento do agente regulado; e (ii) o legislador pátrio optou por apontar "fatores objetivos" e "utilização exclusiva de meios próprios" como critérios cumulativos para a avaliação do "esforço razoável", é necessário que o teor dos §§50-52 seja alterado, de modo que seja esclarecido que, no contexto da LGPD, a análise da eficácia da anonimização é limitada aos meios razoavelmente disponíveis ao agente de tratamento, inclusive quanto a análise dos "esforços razoáveis", ainda que outros meios estejam disponíveis no mercado.

b) Fundamento: em seu item 3.1.3, o Estudo Preliminar fornece proposta de interpretação ao entendimento a respeito da suficiente "irreversibilidade" à luz do art. 12 da LGPD.

Nesse sentido o mencionado guia acertadamente afirma ao se avaliar a irreversibilidade, o *caput* do art. 12 requer que sejam considerados dois requisitos: (*i*) esforços razoáveis; e (*ii*) meios próprios. No entanto, ao descrever os elementos que constituem o "esforço razoável", o Estudo Preliminar, influenciado pela regulação europeia, tratou o conceito de "esforço razoável", como conceito que não fica restrito aos limites do agente regulado, mas observa, também, as práticas disponíveis no mercado.

Ocorre que a redação dada pelo legislador pátrio para conceituar o que considera "esforços razoáveis" não equivale ao entendimento europeu sobre o tema.

Explicamos: O legislador europeu, na Consideranda nº 26, optou por considerar, para fins de conceito de "esforços razoáveis", elementos extrínsecos ou intrínsecos ao agente de tratamento de forma alternativa

(utilizado o termo "quer pelo responsável pelo tratamento, quer por outra pessoa"), conforme se extrai do original em português lusitano[9]:

> *"Os princípios da proteção de dados deverão aplicar-se a qualquer informação relativa a uma pessoa singular identificada ou identificável. Os dados pessoais que tenham sido pseudonimizados, que possam ser atribuídos a uma pessoa singular mediante a utilização de informações suplementares, deverão ser considerados informações sobre uma pessoa singular identificável. Para determinar se uma pessoa singular é identificável, importa considerar todos os meios suscetíveis de ser razoavelmente utilizados, tais como a seleção, quer pelo responsável pelo tratamento quer por outra pessoa, para identificar direta ou indiretamente a pessoa singular. Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica. Os princípios da proteção de dados não deverão, pois, aplicar-se às informações anónimas, ou seja, às informações que não digam respeito a uma pessoa singular identificada ou identificável nem a dados pessoais tornados de tal modo anónimos que o seu titular não seja ou já não possa ser identificado. O presente regulamento não diz, por isso, respeito ao tratamento dessas informações anónimas, inclusive para fins estatísticos ou de investigação".*

Esse não foi o caminho optado pelo legislador pátrio, que ao descrever "esforços razoáveis", no §1º, do art. 12, aponta que o conceito de "esforço razoável" deve considerar, de forma cumulada (uso do "e" no lugar do "ou" para conectar os requisitos), tanto os "fatores objetivos", quanto a "utilização exclusiva de meios próprios":

> *§ 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.*

Em outras palavras: pela opção de redação do legislador pátrio, ainda que uma tecnologia apta a reidentificar o titular esteja razoavelmente disponível no mercado, caso ela não se encontre à disposição do agente de tratamento que praticou o processo de anonimização, não pode ser considerado "meio razoável".

Assim, considerando que (*i*) a interpretação a ser fornecida pela ANPD em seu guia não pode se operar de forma contrária à legislação em detrimento do agente regulado; e (*ii*) o legislador pátrio optou por apontar "fatores objetivos" e "utilização exclusiva de meios próprios" como critérios cumulativos para a avaliação do "esforço razoável", é necessário que o teor dos §§50-52 seja alterado, de modo que seja esclarecido que, no contexto da LGPD, a análise da eficácia da anonimização é limitada aos meios razoavelmente disponíveis ao agente de tratamento, inclusive quanto a análise dos "esforços razoáveis", ainda que outros meios estejam disponíveis no mercado.

6— Comentários ao item 3.3 (§76):

a) Comentário: recomendamos a substituição da frase "A pseudonimização de dados pessoais significa substituir quaisquer características identificáveis dos dados por um pseudônimo, ou seja, um valor que não permite a identificação direta do titular dos dados" por "a pseudonimização de dados pessoais significa substituir, remover ou transformar quaisquer identificadores diretos dos dados".

b) Fundamento: A frase mencionada acima, conforme texto apresentada pelo guia proposto, leva ao entendimento equivocado de que a presença de identificadores indiretos em uma base de dados, por si só, leva à sua descaracterização (ou, pelo menos, dos dados vinculados a esses identificadores) como pseudonimizada. Esse entendimento não está alinhado com as melhores práticas sobre o tema e, em última instância, torna a pseudonimização impossível ou, minimamente, indesejável.

Pseudonimizar, como o próprio Guia proposto apresenta, não é retirar a característica do dado como "dado pessoal"; assim, um dado pseudonimizado precisa ser informação relacionada a uma "*pessoa física identificada ou identificável*".

Assim, para que um dado seja considerado "pseudonimizado" a interpretação mais adequada da legislação é que ele deixe de se referir a uma pessoa "identificada" e passe a se referir a uma pessoa "identificável" — isto é, que para identificar a pessoa seja necessário informação adicional, independente de existirem (ou não) características com o potencial de

identificar as pessoas na base de dados. Nesse sentido segue o *European Data Protection Board*[10]:

> *In practice, pseudonymisation consists in replacing directly identifying data (name, first name, personal number, phone number, etc.) in a data set with indirectly identifying data (alias, sequential number, etc.). It makes it possible to process the data of individuals without being able to identify them in a direct way. However, it is possible to trace the identity of these individuals thanks to the additional data. As such, pseudonymised data is still personal data and is subject to the GDPR. Pseudonymisation is also reversible, unlike anonymisation.*

De igual modo se posiciona a Autoridade de Dados do Reino Unido ("ICO"), em seu Guia sobre Pseudonimização [11]:

> "*At a basic level, pseudonymisation starts with a single input (the original data) and ends with two outputs (the pseudonymised dataset and the additional information). Together, these can reconstruct the original data. However, in relation to the individuals concerned, each output has meaning only in combination with the other. Pseudonymisation therefore refers to techniques that replace, remove or transform information that identifies an individual. For example, replacing one or more identifiers which are easily attributed to individuals (such as names) with a pseudonym (such as a reference number). While you can tie that pseudonym back to the individual if you have access to the additional information, your technical and organisational measures should ensure that you hold this information separately.*"

Assim, a pseudonimização, conforme indicam as supracitadas Autoridades de Dados, deveria ser interpretado como técnica de resguardo ao titular, impossibilitando a sua identificação direta e dificultando a sua identificação indireta, ao pseudonimizar apenas aquelas características que são facilmente atribuídas a um titular em específico.

Ao revés, o guia proposto, ao requerer que toda e qualquer característica "identificável" seja substituída por um pseudônimo, para todos os efeitos práticos, inviabiliza a pseudonimização.

Isso se opera, em primeiro lugar, porque o pseudônimo, pela sua própria natureza, é uma característica identificável. A título de exemplo,

entendemos ser pouco discutível que as informações visíveis de um dado mascarado podem ser utilizadas, em conjunto com outras, para potencialmente se identificar o indivíduo. Logo, substituir uma "característica identificável" por um pseudônimo, nada mais é, senão, substituir uma característica identificável por outra.

Nesse sentido, apesar de o conceito mencionado parecer ser extraído do Guia apresentado pela Autoridade de Dados da Irlanda sobre o tema, sua leitura contextual do leva à conclusão de que ele se refere a informações que permitam a identificação direta do titular, vez que caracteriza o próprio pseudônimo como identificador indireto[12]:

> *"Pseudonymisation" of data means replacing any identifying characteristics of data with a pseudonym, or, in other words, a value which does not allow the data subject to be directly identified.*
> *(...)*
> *Although pseudonymisation has many uses, it should be distinguished from anonymisation, as it only provides a limited protection for the identity of data subjects in many cases as it still allows identification using indirect means. Where a pseudonym is used, it is often possible to identify the data subject by analysing the underlying or related data".*

Em segundo lugar, tornaria a prática de anonimização indesejada, vez que implicaria na inutilidade dos dados da base pseudonimizada. Explicamos: tomemos por exemplo uma base de dados biométrica de clientes de uma dada instituição com quatro atributos: "CPF"; "cor da pele"; "cor dos olhos" e "cor do cabelo".

Seguindo o guia do ICO para pseudonimizar essa base, bastaria, a princípio, que a Instituição em questão substituísse o identificador direto ("CPF") por um pseudônimo (ex. um código *hash* do CPF), vez que os demais dados, por si só, não são aptos a facilmente se identificar um indivíduo. Ocorre que, em sua linguagem atual, isso não poderia se dizer em relação ao Guia proposto pela ANPD, vez que "cor da pele", "cor dos olhos" e "cor do cabelo" são "características identificáveis" e para que a base fosse considerada "pseudonimizada" se faria necessário gerar pseudônimo para cada um desses atributos o que, em última instância, a inutiliza.

Além disso, a frase objeto deste comentário leva, ainda, ao entendimento equivocado de que a única forma de se pseudonimizar adequadamente um dado é pela substituição do identificador por um pseudônimo, o que, conforme extraímos do supramencionado Guia do ICO

não é apropriado, vez que esse resultado pode, igualmente, ser obtido, pela eliminação dos identificadores (ex. digamos que no exemplo acima, muitos dos clientes da instituição possuem combinações únicas, pelo que a Instituição opta por apenas eliminar a coluna "CPF") ou sua alteração (ex. no lugar de substituir o dado "CPF" por um "*Hash*", opta-se por mascará-lo).

Tomando tudo em consideração, recomendamos que a redação da primeira frase do §76 passe a ser: "A pseudonimização de dados pessoais significa substituir, remover ou transformar quaisquer identificadores diretos dos dados".

7– Comentários ao item 3.3 (§84):

a) Comentário: Recomendamos que a frase "algumas etapas devem ser observadas" no §84, seja substituída por "é recomendável que algumas etapas sejam observadas".

b) Fundamento: A expressão "algumas etapas devem ser observadas" leva à conclusão de que a observância do procedimento apresentado pela ANPD é necessária para a execução da uma pseudonimização eficaz ou, minimamente, o desenvolvimento e implementação de metodologia eficaz de pseudonimização. Ocorre que nenhuma das conclusões parece adequada.

Conforme descrito no item anterior, a pseudonimização nada mais é, senão a aplicação de técnicas que, com o objetivo de resguardar o titular, removem ou substituem dados que o identificam, impossibilitando a sua identificação direta e dificultando a sua identificação indireta.

Assim, a aplicação de pseudonimização eficaz independe da observância de processo ou metodologia pré-determinado, desde que o seu resultado seja eficaz – isto é: desde que, em concreto, o risco de identificação ao titular seja significativamente reduzido.

Adicionalmente, embora se reconheça que a observância de uma metodologia seja mecanismo positivo, tanto por permitir avaliar se a técnica empregada é adequada para a situação concreta (isto é, efetivamente reduzindo o risco de identificação do titular), quanto por permitir demonstrar a implementação desta técnica, o termo "devem ser observadas" levam ao entendimento de que apenas a metodologia apresentada pela ANPD se faz adequada para estes fins, o que não é verdade, nem adequado.

Com efeito, podem subsistir outras metodologias de pseudonimização igualmente relevantes, eficazes e úteis, sejam códigos expedidos pela

indústria, como a ABNT NBR ISO 25237:2017 (Informática em saúde – Pseudonimização), sejam expedidas por Autoridades de Dados estrangeiras. A título de exemplo, o ICO, em seu guia sobre o tema, apresenta sua própria metodologia recomendada[13]:

> *"To use pseudonymisation effectively, you must:*
> *– define your goals;*
> *– detail your risks;*
> *– decide on the most appropriate technique; and*
> *– document the outcome"*

Não devendo tais metodologias serem tratadas como menos ineficientes (ou mesmo ineficazes) pelo guia da ANPD. Deste modo, sugerimos que o termo "algumas etapas devem ser observadas" no §84 do Estudo Preliminar, seja substituído por "é recomendável que algumas etapas sejam observadas".

São Paulo (SP), 28 de fevereiro de 2024.

Rony Vainzof[1] | Caio Lima[2] | Jean Santana[3]| Alexandra Lopes[4]

[1] Consultor em Proteção de Dados da FecomercioSP e Sócio-Fundador do VLK Advogados.
[2] Sócio-Fundador do VLK Advogados.
[3] Advogado do VLK Advogados.
[4] Advogada do VLK Advogados.

Referências:

[1] Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/web-guia-anpd-tratamento-de-dados-para-fins-academicos.pdf. Acesso em 16.02.2024

[2] Disponível em: https://www.dataprotection.ie/en/individuals/data-protection-basics/definition-key-terms#:~:text=The%20term%20%E2%80%9Cprocessing%E2%80%9D%20refers%20to,involve%20automated%20or%20manual%20operations. Acesso em 16.02.2024

[3] Disponível em: https://iapp.org/news/a/does-anonymization-or-de-identification-require-consent-under-the-gdpr/. Acesso em 16.02.2024

[4] Disponível em: https://iapp.org/media/pdf/resource_center/wp216_Anonymisation-Techniques_04-2014.pdf. Acesso em 16.02.2024

[5] Disponível em: https://www.aepd.es/en/prensa-y-comunicacion/blog/anonymisation-and-pseudonymisation. Acesso em 16.02.2024

[6] Disponível em: https://iapp.org/media/pdf/resource_center/wp216_Anonymisation-Techniques_04-2014.pdf. Acesso em 16.02.2024

[7] Disponível em: https://ico.org.uk/media/about-the-ico/consultations/2619862/anonymisation-intro-and-first-chapter.pdf. Acesso em 16.02.2024

[8] Disponível em: https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190614%20Anonymisation%20and%20Pseudonymisation.pdf. Acesso em 16.02.2024

[9] Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em 16.02.2024

[10] Disponível em: https://edpb.europa.eu/sme-data-protection-guide/secure-personal-data_en#:~:text=Pseudonymisation%20is%20the%20processing%20of,to%20technical%20and%20organisational%20measures.. Acesso em 16.02.2024

[11] Disponível em: https://ico.org.uk/media/about-the-ico/consultations/4019579/chapter-3-anonymisation-guidance.pdf. Acesso em 16.02.2024

[12] Disponível em: https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190614%20Anonymisation%20and%20Pseudonymisation.pdf. Acesso em 16.02.2024

[13] Disponível em: https://ico.org.uk/media/about-the-ico/consultations/4019579/chapter-3-anonymisation-guidance.pdf. Acesso em 16.02.2024

A Associação Brasileira das Empresas do Mercado de Fidelização ("ABEMF"), vem apresentar os seus comentários à minuta de Estudo Preliminar de Anonimização e Pseudonimização para a proteção de dados pessoais apresentada pela Autoridade Nacional de Proteção de Dados ("ANPD") para consulta à sociedade:

1 – Comentários ao Glossário:

a) Comentário: sugerimos que o conceito de "dado pseudonimizado" passe a constar a possibilidade de uso de *"recurso adicional" para identificar o dado, além de informação, passando a figurar como "Dado que perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação ou recurso adicional mantida separadamente pelo controlador em ambiente controlado e seguro*".

b) Fundamento: ao limitar o dado pseudonimizado de modo que apenas permite a identificação do individuo por intermédio exclusivamente de informação adicional, o Estudo Preliminar não se atenta a possibilidade de que o controlador pode utilizar-se da pseudonimização, mesmo sem diretamente deter os meios pelo qual a informação pode (ou não) ser revertida – por exemplo, o Controlador pode utilizar um serviço de terceiro que permita-lhe encriptar os dados em repouso por si detidos, sem possuir diretamente as chaves de decriptação que lhe permitiriam recuperar a informação originária.

2– Comentários ao Glossário:

a) Comentário: sugerimos que o conceito de "identificar indireto" passe a constar a possibilidade deste identificar não o titular com o uso de informação adicional, mas um "identificador direto" passando a figurar como *"Dado que, por si só, não tem a capacidade de identificar uma pessoa natural, mas pode ser agregado ou vinculado a dados auxiliares para identificar uma pessoa natural ou a identificadores diretos para identificar uma pessoa natural.*".

b) Fundamento: a ANPD deve considerar a possibilidade de que a reversão de um processo de pseudonimização não permita a identificação direta do titular, mas apenas conceda acesso a um identificador direto. Explicamos: embora subsistam identificadores diretos que, razoavelmente, permitam a identificação imediata do titular (como o número do CPF), existem identificadores que, ainda que razoavelmente classificados como diretos, por si só, podem não permitir a identificação imediata do titular – por exemplo, o "nome" do titular, embora

seja considerado um identificador direto, pode não permitir a sua imediata identificação, em caso de existência de homônimos.

3– Comentários ao item 2.2 (§16º):

a) Comentário: para se evitar insegurança jurídica, recomendamos que a ANPD (*i*) reforce o posicionamento no sentido de que a mera possibilidade futura de reidentificação, não afasta a caracterização da informação como anonimizada; (*ii*) reconheça expressamente que a identificação acurada de riscos de reidentificação nem sempre é fácil (ou viável); e (*iii*) pelos motivos elencados, desde que o processo de anonimização se opere de forma razoavelmente robusta, atentando-se às boas-práticas, os dados ser~~ao considerados anonimizados . Para evitar insegurança jurídica, recomendamos que a ANPD fortaleça sua posição, esclarecendo que a mera possibilidade futura de reidentificação não impede a caracterização da informação como anonimizada. Além disso, é crucial que reconheça explicitamente a dificuldade (ou inviabilidade) de identificar precisamente os riscos de reidentificação. Por fim, considerando os motivos apresentados, sugerimos que, desde que o processo de anonimização seja realizado de maneira robusta, em conformidade com as boas práticas, os dados sejam classificados como anonimizados.

b) Fundamento: o §16º, do Estudo Preliminar pode levar ao equivocado entendimento de que a mera possibilidade de reidentificação futura dos titulares descaracteriza o dado enquanto anonimizado – uma consequência indesejável, pois, como bem pontua a própria ANPD em sede do guia sob análise, o risco de reidentificação, por menor que seja, se fará sempre presente (§§41-42, do Estudo Preliminar).

Com efeito, recobramos, o papel do processo de anonimização não é eliminar o risco de reidentificação, mas sim permitir com que este seja substancialmente reduzido (§24º, do Estudo Preliminar).

Outrossim, ao abordar a existência de riscos de reidentificação e sua relação com os dados a ANPD deve partir de uma posição realista de que os riscos de reidentificação não são facilmente identificáveis ou mensuráveis. Nessa esteira, a Autoridade de Dados da Irlanda [1]:

> *"It is not normally possible to quantify the likelihood of re-identification of individuals from anonymised data. However, thinking about the risks which are present will assist in assessing whether identification of data subjects from anonymised data is likely. An effective anonymisation technique will be able to prevent the singling out of individual data subjects, the linking of records or matching of data between data sets, and inference of any information about individuals from a data set".*

Assim, desde que a técnica de anonimização empregada seja, considerando o momento de sua execução, robusta, seguindo-se boas-práticas, seja por intermédio da técnica de gestão de riscos definidas pela ANPD no Estudo Preliminar, sejam outras medidas de mensuração da anonimização reconhecidas como razoavelmente eficazes pelo mercado (como a própria K-Anonimização, exemplificada no Estudo Preliminar).

Desta feita, é forçoso que a ANPD reconheça que o dado deve ser considerado anonimizado, desde que empregada medidas robustas de anonimização razoavelmente reconhecidas como tal pelo mercado, sob pena de gerar grave insegurança jurídica nas organizações quanto a adequação (ou não) das técnicas de anonimização empregadas.

4– Comentários aos §§20 e 25:

a) Comentário: recomendamos que, onde aplicável, especialmente nos §§20° e 25°, do Estudo Preliminar, a ANPD substitua "dado ou informação adicional" por "dado auxiliar".

b) Fundamento: em sede do glossário a ANPD conceituou dado auxiliar, em apertada síntese, como um identificador ou informação adicional que pode ser utilizada para identificar o titular a que se refere o dano anonimizado.

Entretanto, a despeito de sua presença no glossário, o termo jamais foi utilizado no guia no contexto querido pelo glossário: isto é, de pseudonimização. Ao revés, o Estudo Preliminar opta por simplesmente utilizar seu conceito ou sinônimos a este. Uma vez que essa postura pode desincentivar o entendimento e uso da linguagem técnico-jurídica fixada pela própria ANPD, recomendamos que, onde aplicável, especialmente no §20°, a ANPD substitua "dado ou informação adicional" por "dado auxiliar".

5– Comentários ao item 2.2(§22):

a) Comentário: recomendamos que, para se evitar insegurança jurídica, a ANPD esclareça que o direito do titular à anonimização referido no §22, apenas subsiste caso os dados em questão sejam "desnecessários, excessivos ou tratados em desconformidade" com a LGPD.

b) Fundamento: a leitura do §22°, do Estudo Preliminar, em sua redação atual pode levar ao equivocado entendimento de que a Lei Geral de Proteção de Dados conferiu ao titular um direito amplo e geral à anoniminização de seus dados – este, no entanto, seria um entendimento equivocado, que não encontra guarida no texto legal.

Com efeito, a legislação apenas confere ao titular o direito de anonimizar os seus dados em sede do art. 18°, IV – o qual elenca como pré-requisito a esse direito, que os dados que

se busca anonimizar sejam "desnecessários, excessivos ou tratados em desconformidade" com a LGPD.

Desta feita, para se evitar uma interpretação equivocada do referido artigo, que confira ao titular um direito que, em verdade, ele não possui, qual seja: exigir a anonimização de seus dados com base exclusiva em sua vontade, é importante que se destaque os limites legislativos do direito do titular no §22º, do Estudo Preliminar.

6– Comentários ao item 3.1.1 (§§27-32):

a) Comentário: Recomendamos que seja expressamente incluído no item 3.1.1 a possibilidade de fundamentação do processo de anonimização na base legal que fundamentou o tratamento originário, desde que a finalidade da anonimização não seja incompatível com a finalidade da operação de tratamento original".

b) Fundamento: Os §§27-32, do Estudo Preliminar levam o leitor a concluir que toda a carga regulatória aplicável habitualmente a uma operação de tratamento, inclusive a necessidade de fundamentação em uma base legal, se fazem aplicáveis a operação de anonimização, observada isoladamente – isto é, como se o processo de anonimização se perfizesse, por si, uma operação de tratamento – gerando, por conseguinte, a necessidade de fundamentar a operação em uma base legal própria.

Esse entendimento, no entanto, contraria a melhor interpretação jurídica e traz consequências práticas não desejáveis, notadamente o forte desincentivo aos agentes de tratamento em seguir com o processo de anonimização.

Em relação aos aspectos jurídicos, é necessário, antes de tudo, definir o que se entende por "tratamento de dados". Nesse sentido devemos ter em atenção que, apesar de o legislador pátrio ter apresentado rol de atividades exemplificativas isoladas (ex. coleta, produção, utilização...) para descrever o significado de "tratamento de dados", quando essas atividades, em conjunto, integram processo de negócio, ele em sua inteireza deve ser visto como a "atividade de tratamento", não suas partes individualizadas.

Nesse sentido, a norma técnica nacional ABNT NBR ISO 29100:2020[2] conceitua tratamento de dados pessoais como "*operação ou conjunto de operações realizadas sobre dados pessoais*". Em igual sentido se posiciona a Autoridade de Dados da Irlanda [3]:

> *"The term "processing" refers to any operation or set of operations performed on personal data. Processing includes storing, collecting, retrieving, using, combining, erasing and destroying personal data, and can involve automated or manual operations".*

O entendimento é relevante pois ele define "o que" deve ser objeto da conformidade com a legislação: a "ação" avaliada isoladamente ou o processo, avaliado em seu todo. Do nosso lado, entendemos que o processo, em sua inteireza, deve ser considerado para a avaliação da conformidade regulatória — ou seja: ainda que uma "base legal" possa não parecer adequada para uma "ação" específica, se ela for adequada ao processo que a ação integra, ela pode ser utilizada para justificar a ação, pois a "atividade de tratamento" é o processo como um todo, não as partes isoladas que o compõem.

Concluir de forma diversa seria negativo, tornando mesmo as obrigações mais simples da legislação, como o registro de operações de tratamento (Art. 37, da LGPD), inexequíveis vez que cada ação individual que compõe cada processo precisaria ser objeto de registro próprio, de teste de balanceamento próprio, de Relatório de Impacto próprio e assim sucessivamente, os quais precisariam ser acompanhados e geridos em sua individualidade — o que certamente é impossível para todas as organizações, independentemente do porte.

Adicionalmente, mesmo garantir a licitude dos processos internos pode ser impossível, seja porque algumas ações apenas podem se adequar à legislação quando entendidas à luz de seus respectivos processos, seja porque inexiste suficiente mão de obra para atender aos requisitos de licitude de cada ação individualizada (ex. realizar o teste de balanceamento para cada uma das atividades).

Nessa linha, a atividade de anonimização não deve ser encarada como operação de tratamento individualizada, mas como parte integrante de operação de tratamento prévia: aquela que justifica a detenção dos dados pelo agente de tratamento. Mais precisamente: a anonimização deve ser encarada como o ato de encerramento da operação de tratamento, sendo alternativa à eliminação dos dados

Esse foi o entendimento do legislador pátrio ao apontar a anonimização de dados como alternativa à eliminação dos dados, nos termos do art. 16, IV, da LGPD.

Nesse sentido também o posicionamento da Autoridade de Dados da Itália, em seu guia sobre programas de fidelidade, ao mencionar a anonimização como forma de retenção dos dados, após atingida a finalidade do seu tratamanto [4]:

> *The principle to be abided by is that any personal data that does not need to be retained for the purposes for which it has been processed must be either erased or anonymised (see Section 11(1), letter e), of the Code).*

Ainda que a atividade de anonimização não se destine a encerrar a operação de

tratamento, mas criar cópia anonimizada dos dados, de modo a permitir que eles sejam utilizados de uma forma que, não fosse a anonimização, a atividade de tratamento não seria adequada (seja por implicações de segurança, seja pela ausência de fundamento legal específico), entendemos que o processo da anonimização poderá ocorrer conforme a base legal originária, desde que seja compatível com a finalidade para a qual o dado foi originalmente coletado (e entendemos que isso é o que ocorrerá como regra). Nesse sentido, El Emam e Hintze, em artigo escrito para a IAPP[5]:

> *"In other words, the processing of personal data in order to fully anonymize it is "compatible with the purpose for which the personal data are initially collected" and therefore does not require an additional legal basis, such as consent, specifically for the act of anonymizing".*

Essa é a interpretação teleológica mais adequada ao art. 9º, §2º, da LGPD, que embora se refira ao consentimento, é razoavelmente adequada a qualquer outra base legal: do mesmo modo que a necessidade de oportunizar a revogação do consentimento apenas é requerida se a finalidade for incompatível com a do consentimento originário, a necessidade de nova fundamentação da operação de tratamento também apenas deve ser necessária se a nova finalidade for incompatível.

Ainda, a conclusão em questão é lógica e necessária do ponto de vista prático: se a operação de anonimização precisa ser fundamentada em nova base legal (em grande parte dos casos, sobretudo em caso de envolvimento de dados pessoais sensíveis, a base legal seria o consentimento), os agentes de tratamento serão desincentivados a adotar o processo de anonimização, vez que isso agregará custo significativo, sem que nenhum benefício real advenha para o agente de tratamento em questão, o que, por sua vez, acresce riscos aos titulares.

Esse ponto apresentado está em linha com as disposições do CNIL, que, a título de exemplo, já prevendo tanto que (*i*) a anonimização habitualmente é feita para situações em que o tratamento não seria adequado de outra maneira; (*ii*) é utilizado como alternativa à eliminação, findo o período de retenção [6]:

> "*De fato, a anonimização abre potencial para a reutilização de dados que inicialmente era proibido devido à natureza pessoal dos dados usados e, portanto, permite que os atores explorem e compartilhem seu 'depósito' de dados sem infringir a privacidade das pessoas. Ele também permite que os*

dados sejam retidos além de seu período de retenção". (tradução livre)

Diante disso, recomendamos que seja expressamente incluída no item 3.1.1 a possibilidade de fundamentação do processo de anonimização na base legal que fundamentou o tratamento originário, desde que a finalidade da anonimização não seja incompatível com a finalidade da operação de tratamento original".

7– Comentários ao item 3.1.1 (§§33-37):

a) Comentário: Visando garantir a segurança jurídica, propomos que seja claramente incorporada à seção 3.1.1 o seguinte texto: "Em termos gerais, presume-se que a anonimização seja compatível com a finalidade original do tratamento".

b) Fundamento: Reconhecendo a importância crucial da harmonização de todos os procedimentos relacionados ao tratamento de dados pessoais com as finalidades originalmente comunicadas aos titulares, visando evitar a instauração de insegurança jurídica, é imperativo esclarecer, como regra, a compatibilidade das operações de anonimização com os propósitos iniciais, ressalvadas circunstâncias absolutamente excepcionais.

Isso se fundamenta na compreensão de que, em primeiro lugar, a prática da anonimização representa medida que objetiva, ou no mínimo, possui como efeito necessário, conferir maior segurança aos titulares de dados – vez que reduz de forma considerável o risco de identificação dos titulares, prevenindo, consequentemente, a sua exposição a incidentes ou irregularidades durante o processo de tratamento.

Além disso, a prática da anonimização se configura como ferramenta essencial para a observância do princípio da necessidade em seu aspecto temporal, ou seja, para evitar a retenção de dados pessoais em formato identificável por período além do estritamente necessário.

Nesse sentido é o posicionamento do *European Data Protection Board* (a época, Article 29 *Working Party*) em seu guia sobre o tema [7]:

> *"On the other hand, the provisions contained in Article 6(1) e) of the Directive 95/46/EC (but also in Articles 6(1) and 9(1) of the e-Privacy Directive) ought to be pointed out as they demonstrate the need to keep personal data "in a form which permits identification" for no longer than is necessary for the purposes of the collection or further processing. In itself, this provision makes a strong point that personal data should, at least, be anonymised "by*

default" (subject to different legal requirements, such as those mentioned in the e-Privacy Directive regarding traffic data). If the data controller wishes to retain such personal data once the purposes of the original or further processing have been achieved, anonymisation techniques should be used so as to irreversibly prevent identification. Accordingly, the Working Party considers that anonymisation as an instance of further processing of personal data can be considered to be compatible with the original purposes of the processing but only on condition the anonymisation process is such as to reliably produce anonymised information in the sense described in this paper"

Na mesma linha, e com base na opinião acima, a Autoridade de Dados da Espanha[8]:

"*The processing activity that produces anonymised data is a processing of personal data, which can be considered to be compatible with the original purposes of processing from which the data are obtained*"

No mesmo sentido, recordamos a posição do CNIL[9]::

"*De fato, a anonimização abre um potencial para a reutilização de dados que inicialmente era proibido devido à natureza pessoal dos dados usados e, portanto, permite que os atores explorem e compartilhem seu "depósito" de dados sem infringir a privacidade das pessoas. Ele também permite que os dados sejam retidos além de seu período de retenção*". (tradução livre)

Tudo considerado, recomendamos que, para garantia da segurança jurídica, seja claramente incorporada à seção 3.1.1 o seguinte trecho: "Em termos gerais, presume-se que a anonimização seja compatível com a finalidade original do tratamento".

8– Comentários ao item 3.1.1 (§§38-40):

a) Comentário: Recomendamos a exclusão dos §§38-40 do Guia e a inserção de um esclarecimento indicando que "a anonimização e a pseudonimização são estratégias que o agente de tratamento pode empregar para cumprir o princípio da necessidade".

b) Fundamento: Nos §§38-40 do Estudo Preliminar em análise, a ANPD indica que o processo de anonimização necessita passar por prévia validação à luz do princípio da necessidade.

Ao nosso entender, entretanto, essa orientação deve ser eliminada, uma vez que o processo de anonimização é ferramenta que concretiza o princípio da necessidade, não fazendo sentido

que, de forma prévia à sua aplicação se imponha estudo preliminar sobre a aplicação desse princípio.

Como bem pontua o *European Data Protection Board*, no posicionamento acima exposto, a anonimização "por *default*" nada mais é do que o atendimento ao dever de não reter os dados pessoais para além do tempo estritamente necessário. Recordamos[10]:

> *"On the other hand, the provisions contained in Article 6(1) e) of the Directive 95/46/EC (but also in Articles 6(1) and 9(1) of the e-Privacy Directive) ought to be pointed out as they demonstrate the need to keep personal data "in a form which permits identification" for no longer than is necessary for the purposes of the collection or further processing. In itself, this provision makes a strong point that personal data should, at least, be anonymised "by default" (subject to different legal requirements, such as those mentioned in the e-Privacy Directive regarding traffic data)."*

Outrossim, se tratando, o processo de anonimização, de uma indubitável operação voltada a minimização de dados, seja de forma estratégica, seja como consequência necessária do processo em si, este naturalmente atenderá ao princípio da necessidade, em relação ao qual a minimização de dados é corolário, de modo que referida "avaliação preliminar da necessidade" se converterá em mera formalidade.

Nesse sentido, a Autoridade de Dados do Reino Unido destaca o papel da anonimização em apoiar o atendimento do princípio da "minimização de dados"[11]:

> "*Anonymisation limits your data protection risks, and can enable you to make information available to other organisations or to the public. It also supports the principle of data minimisation. If you process personal data, you have to comply with the data protection principles and be able to demonstrate how you do so. The principles regulate the disclosure of personal data and establish a framework through which you can do this fairly, lawfully and transparently*".

Em igual sentido, a Autoridade de Dados da Irlanda pontua a possibilidade de utilização da anonimização de dados como parte da estratégia de *privacy by design* ou de minimização de dados, mesmo quando a anonimização não é efetiva [12]:

> "*In some cases, it is not possible to effectively anonymise data, either because of the nature or context of the data, or because of the use for which the data is collected and retained. Even in these circumstances, organisations might want to use anonymisation or pseudononymisation techniques:- 1. As part of a "privacy by design" strategy to provide improved protection for data subjects 2. As part of a risk minimisation strategy when sharing data with data*

processers or other data controllers. 3. To avoid inadvertent data breaches occurring when your staff is accessing personal data. 4. As part of a "data minimisation" strategy aimed at minimising the risks of a data breach for data subjects".

Assim, entendemos que, no lugar de submeter o processo de anonimização a verificação prévia de sua compatibilidade com o princípio da necessidade – o que, em regra, se revelará não apenas processo burocrático sem real sentido, mas também como desincentivo a se seguir com a anonimização – a ANPD deve destacar o papel de anonimização e da pseudonimização na estratégia de minimização de dados.

Diante disso, recomendamos a exclusão dos §§38-40 do Guia e a inserção de esclarecimento indicando que "a anonimização e a pseudonimização são estratégias que o agente de tratamento pode empregar para cumprir o princípio da necessidade".

9– Comentários ao item 3.1.2 (§42):

a) Comentário: Visando garantir a segurança jurídica, propomos que, em sede do §42º, do Estudo Preliminar, o termo "dado auxiliar", seja substituído por "informação publicamente disponível".

b) Fundamento: o §42º, do Estudo Preliminar, ao buscar explicar a existência de riscos de reidentificação presentes em dados que, para fins jurídicos, são reconhecidamente anonimizado, emprega o termo "dado auxiliar" para referir-se a míriade de informações constantes na internet, que poderiam (em teoria) ser utilizados em ataques de reidentificação – isto é, ações com o objetivo de reverter o processo de deidentificação.

O uso do termo neste contexto, no entanto, parece-nos técnicamente inadequado ao conceito a ele conferido pelo Estudo Preliminar, podendo levar, inclusive, a uma inadequada confusão entre anonimização e pseudonimização.

Para explicar nossa posição, é necessáiro, antes de tudo, observar que em seu glossário, o Estudo Preliminar vincula o conceito de "dado auxiliar" ao conceito de "pseudonimização" – com efeito, dado auxiliar seria, justamente, a informação adicional, mantida apartada pelo Controlador, que possibilitaria a identificação do titular, cujos identificadores direitos foram transformados em pseudônimos ou eliminados.

Desta feita, ao utilizar o termo "dado auxiliar" dentro do contexto de anonimização, o Estudo Preliminar leva a inerente confusão entre os conceitos de "anonimização" e "pseudonimização".

Ainda que se entenda que o objetivo do paragráfo em questão é demonstrar a inexistência de dado "absolutamente anonimizado" – isto é, a persistência do risco de

reidentificação do dado anonimizado, ainda que significativamente inferior àquele de um dado considerado meramente pseudonimizado —, seria mais apropriado falar em "informações publicamente disponíveis", não "dados auxiliares", porquanto sugere-se a alteração do termo.

10— Comentários ao item 3.1.2 (§42):

a) Comentário: Visando garantir a segurança jurídica, propomos que, em sede do §42º, do Estudo Preliminar, o termo "dado auxiliar", seja substituído por "informação publicamente disponível".

b) Fundamento: o §42º, do Estudo Preliminar, ao buscar explicar a existência de riscos de reidentificação presentes em dados que, para fins jurídicos, são reconhecidamente anonimizado, emprega o termo "dado auxiliar" para referir-se a míriade de informações constantes na internet, que poderiam (em teoria) ser utilizados em ataques de reidentificação — isto é, ações com o objetivo de reverter o processo de deidentificação.

O uso do termo neste contexto, no entanto, parece-nos técnicamente inadequado ao conceito a ele conferido pelo Estudo Preliminar, podendo levar, inclusive, a uma inadequada confusão entre anonimização e pseudonimização.

11— Comentários ao item 3.1.3 (§§50-52):

a) Comentário: Considerando que (i) a interpretação do guia da ANPD não pode contrariar a lei em prejuízo do agente regulado; e (ii) o legislador nacional indicou "fatores objetivos" e "uso exclusivo de meios próprios" como critérios cumulativos para avaliar o "esforço razoável", é preciso modificar os §§50-52 de modo a esclarecer que, na LGPD, a avaliação da eficácia da anonimização se restringe aos meios razoavelmente disponíveis ao agente de tratamento, incluindo a análise dos "esforços razoáveis", mesmo que outros meios estejam disponíveis no mercado.

b) Fundamento: Em seu item 3.1.3, o Estudo Preliminar fornece proposta de interpretação ao entendimento a respeito da suficiente "irreversabilidade" à luz do art. 12º, da LGPD.

Nesse sentido, o mencionado guia acertadamente firma a necessidade de atender a dois requisitos: (i) esforços razoáveis; e (ii) meios próprios. Entretanto, ao abordar os elementos que compõem o "esforço razoável", o Estudo Preliminar, influenciado pela regulação europeia, interpreta esse conceito como não restrito aos limites do agente regulado, considerando as práticas disponíveis no mercado como suficientes para atendê-los.

No entanto, a redação atribuída pelo legislador nacional para definir o termo "esforços razoáveis" não coincide com a compreensão europeia sobre o assunto. Explicando de maneira

mais detalhada: enquanto o legislador europeu, na Consideranda nº 26, escolheu considerar, para a definição de "esforços razoáveis", elementos tanto extrínsecos quanto intrínsecos ao agente de tratamento de maneira alternativa (utilizando a expressão "quer pelo responsável pelo tratamento, quer por outra pessoa"), conforme se depreende do texto original em português lusitano[13]:

> *"Os princípios da proteção de dados deverão aplicar-se a qualquer informação relativa a uma pessoa singular identificada ou identificável. Os dados pessoais que tenham sido pseudonimizados, que possam ser atribuídos a uma pessoa singular mediante a utilização de informações suplementares, deverão ser considerados informações sobre uma pessoa singular identificável. Para determinar se uma pessoa singular é identificável, importa considerar todos os meios suscetíveis de ser razoavelmente utilizados, tais como a seleção, quer pelo responsável pelo tratamento quer por outra pessoa, para identificar direta ou indiretamente a pessoa singular. Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica. Os princípios da proteção de dados não deverão, pois, aplicar-se às informações anónimas, ou seja, às informações que não digam respeito a uma pessoa singular identificada ou identificável nem a dados pessoais tornados de tal modo anónimos que o seu titular não seja ou já não possa ser identificado. O presente regulamento não diz, por isso, respeito ao tratamento dessas informações anónimas, inclusive para fins estatísticos ou de investigação".*

Esse não foi o caminho optado pelo legislador brasileiro, que ao descrever "esforços razoáveis", no §1º, do art. 12º, aponta que o conceito de "esforço razoável" deve considerar, de forma cumulada (uso da locução coordenativa aditiva "e" no lugar da locução coordenativa alternativa "ou" para conectar os requisitos), tanto os "fatores objetivos", quanto a "utilização exclusiva de meios próprios":

> *§1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.*

Em outras palavras: pela opção de redação do legislador pátrio, ainda que uma tecnologia apta a reidentificar o titular esteja razoavelmente disponível no mercado, caso ela não se encontre razoavelmente à disposição do agente de tratamento que praticou o processo de anonimização, não pode ser considerado "meio razoável".

Assim, considerando que (i) a interpretação do guia da ANPD não pode contrariar a lei em prejuízo do agente regulado; e (ii) o legislador nacional indicou "fatores objetivos" e "uso exclusivo de meios próprios" como critérios cumulativos para avaliar o "esforço razoável", é preciso modificar os §§50-52 de modo a esclarecer que, na LGPD, a avaliação da eficácia da anonimização se restringe aos meios razoavelmente disponíveis ao agente de tratamento, incluindo a análise dos "esforços razoáveis", mesmo que outros meios estejam disponíveis no mercado.

12- Comentários ao item 3.2 (§§56 e 57):

a) Comentário: é relevante que as discussões a respeito do processo de anonimização a que se refere os §§ §56º e 57º, levem em consideração, também, outros fatores objetivos relevantes em sua avaliação, como os custos para a organização, seu porte, e esforços razoáveis empregados.

b) Fundamento: ao se avaliar o emprego de técnicas de anonimização é relevante que critérios objetivos razoáveis sejam discutidos, sobretudo para não alienar agentes de tratamento de menor poder econômico, inclusive agentes de tratamento de pequeno porte.

Com efeito, caso, ao se avaliar a anonimização, não se considere as capacidades econômicas do agente regulado, os custos das técnicas de anonimização disponíveis e os esforços razoáveis empreendidos pelo agente de tratamento, na prática, se excluíra dos agentes de tratamento de pequeno e médio porte a possibilidade de anonimizar os dados e, com isso, utilizá-los com maior liberdade, inclusive em proveito de sua atividade econômica.

Isso se opera porque naturalmente os recursos disponíveis para anonimizar ou reidentificar um determinado registro, serão distintos para os diferentes agentes de tratamento, de modo que uma base de dados.

Com efeito, uma base de dados que pode ser absolutamente deidentificada para a realidade de uma pequena *startup*, poderá ser facilmente reidentificada por uma *bigtech* – uma vez que os recursos tecnológicos e financeiros detidos por esta são incomparavelmente superiores àqueles detidos pela primeira.

Tratar, no entanto, essa base de dados em posse da pequena *startup* como meramente pseudonimizada, sujeitando os agentes de tratamento em posições absolutamente diferentes

ao mesmo tratamento, é inviabilizar a anonimização para aqueles de pequeno e médio porte — vez que passariam a estar sujeitos às técnicas de anonimização e reidentificação mais avançadas disponíveis em mercado, os quais estes, bem provavelmente, sequer possuiriam recursos suficientes para acessar.

13— Comentários ao item 3.3 (§76):

a) Comentário: Recomendamos substituir a seguinte expressão do Guia proposto: "A pseudonimização de dados pessoais significa substituir quaisquer características identificáveis dos dados por um pseudônimo, ou seja, um valor que não permite a identificação direta do titular dos dados" por "A pseudonimização de dados pessoais consiste em substituir, remover ou transformar quaisquer identificadores diretos dos dados".

b) Fundamento: A afirmação acima no Guia proposto pode induzir a interpretação equivocada. Ela sugere erroneamente que a mera presença de identificadores indiretos em uma base de dados resultaria na sua descaracterização como pseudonimizada, ou pelo menos dos dados associados a esses identificadores. Essa interpretação parece não estar alinhada com as melhores práticas no assunto e, em última análise, pode dar a impressão de que a pseudonimização é impossível ou, no mínimo, indesejável.

Pseudonimizar, como o próprio guia proposto apresenta, não é retirar a característica do dado como "dado pessoal"; assim, um dado pseudonimizado precisa ser informação relacionada a "*pessoa física identificada ou identificável*".

Nesse contexto, a interpretação mais apropriada da legislação é que, para que um dado seja considerado "pseudonimizado", ele deve deixar de se referir a uma pessoa "identificada" e passar a se referir a uma pessoa apenas "identificável".

Em outras palavras: um dado deve ser considerado "pseudonimizado" se ausentes identificadores diretos. Esse, reforçamos, não é entendimento novo, mas já foi exposto pelas Autoridades de Dados Europeias.

Nesse sentido, a Autoridade de Dados do Reino Unido, em seu guia sobre pseudonimização [14]:

> "*At a basic level, pseudonymisation starts with a single input (the original data) and ends with two outputs (the pseudonymised dataset and the additional information). Together, these can reconstruct the original data. However, in relation to the individuals concerned, each output has meaning only in combination with the other. Pseudonymisation therefore refers to techniques that replace, remove or transform information that identifies an individual. For example, replacing one or more identifiers which are easily*

attributed to individuals (such as names) with a pseudonym (such as a reference number). While you can tie that pseudonym back to the individual if you have access to the additional information, your technical and organisational measures should ensure that you hold this information separately."

De igual modo, o próprio *European Data Protection Board*[15]:

"In practice, pseudonymisation consists in replacing directly identifying data (name, first name, personal number, phone number, etc.) in a data set with indirectly identifying data (alias, sequential number, etc.). It makes it possible to process the data of individuals without being able to identify them in a direct way. However, it is possible to trace the identity of these individuals thanks to the additional data. As such, pseudonymised data is still personal data and is subject to the GDPR. Pseudonymisation is also reversible, unlike anonymisation".

Por sua vez, a Autoridade de Dados da Itália, em seu guia sobre programas de Fidelidade, embora não faça uso do termo "pseudonimização", claramente a ele faz referência ao abordar o tema de "identificar dados indiretamente", como opção à anonimização[16]:

"Pursuant to the data minimisation principle (Section 3 of the Code), information systems and software shall have to be configured from the start in such a way as to minimise use of information relating to identifiable customers. Personal data related to customers may not be processed if the purposes of the processing – with particular regard to profiling activities – can be achieved by means of either anonymised data or indirectly identifying data;".

Dessa maneira, a pseudonimização, como indicam as Autoridades de Dados mencionadas, deveria ser interpretada como técnica destinada a resguardar o titular, impedindo sua identificação direta e dificultando a identificação indireta, ao pseudonimizar apenas aquelas características facilmente atribuídas a titular específico.

Por outro lado, o guia proposto, ao exigir a substituição de toda e qualquer característica "identificável" por um pseudônimo, na prática, compromete a eficácia da pseudonimização. Isso ocorre, primeiramente, porque o próprio pseudônimo, por sua natureza, é característica identificável. A título de exemplo, é incontestável que as informações visíveis de um dado pseudonimizado podem ser utilizadas, em conjunto com outras, para potencialmente

identificar o indivíduo. Portanto, substituir uma "característica identificável" por pseudônimo equivale, essencialmente, a trocar uma característica identificável por outra.

Nesse contexto, é importante observar que, embora o conceito mencionado provavelmente ser derivado do guia apresentado pela Autoridade de Dados da Irlanda sobre o tema, análise contextual do guia leva à conclusão incontestável de que ele se refere a informações que possibilitam a identificação direta do titular, uma vez que caracteriza o próprio pseudônimo como identificador indireto.

O guia proposto, ao requerer que toda e qualquer característica "identificável" seja substituída por pseudônimo, para todos os efeitos práticos, inviabiliza a pseudonimização.

Isso se opera, em primeiro lugar, porque o pseudônimo, pela sua própria natureza, é característica identificável. A título de exemplo, parece-nos pouco discutível que as informações visíveis de um dado mascarado podem ser utilizadas, em conjunto com outras, para potencialmente se identificar o indivíduo. Logo, substituir uma "característica identificável" por um pseudônimo, nada mais é, senão, substituir uma característica identificável por outra.

Nesse sentido, apesar de o conceito mencionado parecer ter sido extraído do guia apresentado pela Autoridade de Dados da Irlanda sobre o tema, leitura contextual do guia leva à conclusão de que este se refere a informações que permitam a identificação direta do titular, vez que caracteriza o próprio pseudônimo como identificador indireto[17]:

> *"Pseudonymisation" of data means replacing any identifying characteristics of data with a pseudonym, or, in other words, a value which does not allow the data subject to be directly identified.*
>
> *(...)*
>
> *Although pseudonymisation has many uses, it should be distinguished from anonymisation, as it only provides a limited protection for the identity of data subjects in many cases as it still allows identification using indirect means. Where a pseudonym is used, it is often possible to identify the data subject by analysing the underlying or related data".*

Em segundo lugar, tornaria, na prática, a pseudonimização indesejada, vez que implicaria na inutilidade dos dados da base pseudonimizada – vez que a eliminação de identificadores indiretos tende a inutilizar a base, desprovendo-a de suas informações úteis.

Não obstante tudo o que foi mencionado anteriormente, a frase em foco neste comentário

ainda sugere erroneamente que a única maneira adequada de pseudonimizar um dado é através da substituição do identificador por um pseudônimo. No entanto, como destacamos no Guia do ICO anteriormente mencionado, essa abordagem não é a única apropriada. Podem ser alcançados resultados similares por meio da eliminação dos identificadores (por exemplo, em uma base de dados cujo único identificador direto utilizado é o número de CPF, bastaria eliminar a coluna "CPF") ou por meio de sua modificação (por exemplo, mascarar identificadores diretos).

Tomando tudo em consideração, recomendamos substituir a seguinte expressão do guia proposto: "A pseudonimização de dados pessoais significa substituir quaisquer características identificáveis dos dados por um pseudônimo, ou seja, um valor que não permite a identificação direta do titular dos dados" por "A pseudonimização de dados pessoais consiste em substituir, remover ou transformar quaisquer identificadores diretos dos dados".

14– Comentários ao item 3.3 (§81):

a) Comentário: Recomendamos que texto contido no balão azul do §81, passe a constar com a seguinte redação "*Criptografia pode ou não ser anonimização, conforme a existência (ou não) de uma chave de decriptação. Quando a informação original se encontra acessível, as transformações aplicadas pelos algoritmos criptográficos são projetadas para serem reversíveis, no que é conhecido como descriptografia. Neste cenário a Criptografia é uma técnica de pseudonimização. Entretanto, vários algoritmos criptográficos (simétricos, assimétricos e de hash) podem realizar processamentos unidirecionais. Nesses casos atendem os requisitos da anonimização, desde que os dados cifrados sejam úteis*".

b) Fundamento: não se trata de uma alteração de conteúdo, apenas uma proposta de redação com o objetivo de tornar o conteúdo já apresentado mais claro: isto é, que a criptografia poderá (ou não) ser considerada anonimização, em acordo com a sua reversibilidade.

15– Comentários ao item 3.3 (§83):

a) Comentário: Recomendamos que o Estudo Preliminar destaque que, o processo de anonimização por si proposto, embora válido e adequado, não é único, inexistindo impeditivo para o uso independente e exclusivo de outras práticas reconhecidamente eficazes, como a própria K-Anonimização.

b) Fundamento: Para se evitar um entendimento equivocado do Estudo Preliminar em análise, que leve a interpretação de que o uso da técnica de gerenciamento de riscos proposta

é a única metodologia aceitável para a anonimização eficaz, sugerimos que seja destacado que o procedimento é meramente uma sugestão.

Com efeito, é premente que o Estudo Preliminar reconheça que o emprego adequado de qualquer técnica reconhecidamente eficaz para reduzir substancialmente o risco de reidentificação seja suficiente para o reconhecimento do dado como anonimizado.

Com efeito, as próprias metodologias de anonimização citadas pelo Estudo Preliminar, podem ser aplicadas de formas eficazes e independente do modelo de gestão de risco proposto.

Arguir de forma diversa, além de gerar um risco de retrabalho desnecessário – em que as organizações que já dispenderam recursos com a implementação de técnicas reconhecidas, necessitariam executar o processo determinado pela ANPD, não em benefício do titular, mas para mero cumprimento de determinação burocrática – poderá gerar entraves significativos no fluxo internacional de dados, visto que uma informação razoavelmente entendida como anonimizada no estrangeiro, passaria a não o ser no Brasil.

A título de exemplo, a ANPD cita, dentre suas metodologias de anonimização, a técnica "K-anonimização", inclusive, empregando-a em conjunto com a técnica de Gestão de Riscos no apêndice IV. Transcorre que a técnica de K-Anonimização, além de ser medida destinada a implementação da anonimização, é destinada, sobretudo, a verificação do risco de reidentificação, como bem pontua a Autoridade de Dados de Singapura [18]:

> *"K-anonymity (and similar extensions to it like L-diversity and T-closeness) is sometimes thought of as an anonymisation technique, but it is more of a measure used to ensure that risk threshold has not been surpassed, as part of the anonymisation methodology (see in particular step 6). 16.2. K-anonymity is not the only measure available nor is it without its limitations but it is relatively well understood and easy to apply. Alternative methods such as differential privacy9 have emerged over the past few years"*

Assim, quando possível aplicar a K-anonimização em sua completude (isto é, garantir que cada registro possua, pelo menos, um registro idêntico), a técnica de Gestão de Riscos apresentadas, embora válida, se mostraria, para a ampla maioria das organizações, uma completa redundância.

Antes, ela deve ser vista como técnica útil para aquelas situações em que outras metodologias mais simples não possam ser completamente empregadas – é o caso, por

exemplo, do apêndice IV, em que nem todos os registros da base estruturada apresentam um par.

Tudo posto, recomendamos que o Estudo Preliminar destaque que, o processo de anonimização por si proposto, embora válido e adequado, não é único, inexistindo impeditivo para o uso independente e exclusivo de outras práticas reconhecidamente eficazes, como a própria K-Anonimização.

16— Comentários ao item 3.3 (§84):

a) Comentário: Recomendamos que a frase "algumas etapas devem ser observadas" no §84, seja substituída por "Recomenda-se a observação de algumas etapas".

b) Fundamento: A expressão "algumas etapas devem ser observadas" sugere, de forma não precisa, a necessidade estrita de seguir o procedimento delineado pela ANPD para alcançar pseudonimização eficaz ou, no mínimo, para desenvolver e implementar metodologia de pseudonimização. Contudo, nenhuma dessas conclusões se mostra apropriada.

Conforme apresentado no item anterior, a pseudonimização consiste na aplicação de técnicas destinadas a preservar o titular, eliminando ou substituindo dados que o identificam, impedindo sua identificação direta e dificultando a identificação indireta. Assim, a eficácia da pseudonimização não está vinculada à adesão a processo ou metodologia predefinida, desde que o resultado alcançado seja eficaz – ou seja, desde que, na prática, o risco de identificação do titular seja substancialmente reduzido.

Embora se reconheça que a adesão a uma metodologia seja instrumento positivo, permitindo avaliar se a técnica empregada é verdadeiramente apropriada para a situação concreta (ou seja, se reduz efetivamente o risco de identificação do titular) e possibilitando demonstrar a implementação desta técnica, o termo "devem ser observadas" induz à interpretação de que apenas a metodologia apresentada pela ANPD seria adequada para esse propósito, o que não é verídico nem apropriado.

De fato, podem existir outras metodologias de pseudonimização igualmente relevantes, eficazes e úteis, sejam normatizadas pela indústria, como a ABNT NBR ISO 25237:2017 (Informática em saúde — Pseudonimização), ou expedidas por Autoridades de Dados estrangeiras. A título exemplificativo, o ICO, em seu guia sobre o tema, apresenta sua própria metodologia recomendada. [19]:

> *"To use pseudonymisation effectively, you must:*
> *– define your goals;*
> *– detail your risks;*
> *– decide on the most appropriate technique; and*
> *– document the outcome"*

Em igual sentido, a Autoridade de Dados da França[20]:

> "Para construir um processo de anonimização relevante, é aconselhável:
>
> - Identificar as informações a serem mantidas de acordo com sua relevância.
> - remover elementos de identificação direta, bem como valores raros que poderiam permitir a fácil reidentificação de pessoas (por exemplo, a presença da idade dos indivíduos pode tornar muito fácil a reidentificação de centenários);
> - Distinguir informações importantes de informações secundárias ou desnecessárias (ou seja, excluíveis).
> - Defina a delicadeza ideal e aceitável para cada informação retida." (tradução livre).

Não devendo tais metodologias serem tratadas como menos ineficientes (ou mesmo ineficazes) pelo guia da ANPD. Deste modo, sugerimos que o termo "algumas etapas devem ser observadas" no §84 do Estudo Preliminar, seja substituído por "recomenda-se a observação de algumas etapas".

17– Comentários ao apêndice II:

a) Comentário: a técnica de função hash deve ser removida do rol de técnicas voltadas a e pseudonimização e incluída no rol de técnicas voltadas à anonimização.

b) Fundamento: a presença da técnica de função hash no quadro de exemplos de técnicas de pseudonimização representa uma contradição interna no próprio Estudo Preliminar, uma vez que o mesmo reconhece que técnicas de criptografia unidirecional são técnicas de anonimização (§81, do Estudo Preliminar).

Nessa esteira, reforçamos que o risco de quebra da criptografia empregada (ou seja, de reidentificação do dado) não é, por si só, fator para descaracterizar a técnica como técnica de anonimização, vez que o risco de reidentificação encontrar-se-á sempre presente, como, aliás, igualmente, assevera o próprio Estudo Preliminar (§42º, do Estudo Preliminar).

Assim, para se evitar uma contradição lógica, é forçoso que a técnica de função hash deve ser removida do rol de técnicas voltados a técnicas de pseudonimização e incluída no rol de técnicas voltadas à anonimização

São Paulo, 28 de Fevereiro de 2024

Referências:

[1] Disponível em: https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190614%20Anonymisation%20and%20Pseudonymisation.pdf. Acesso em 16.02.2024

[2] Disponível em: https://www.normas.com.br. Acesso em 21.02.2024

[3] Disponível em: https://www.dataprotection.ie/en/individuals/data-protection-basics/definition-key-terms#:~:text=The%20term%20%E2%80%9Cprocessing%E2%80%9D%20refers%20to,involve%20automated%20or%20manual%20operations. Acesso em 16.02.2024

[4] Disponível em: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1109624. Acesso em 22.02.2024

[5] Disponível em: https://iapp.org/news/a/does-anonymization-or-de-identification-require-consent-under-the-gdpr/. Acesso em 16.02.2024

[6] Disponível em: https://www.cnil.fr/fr/lanonymisation-de-donnees-personnelles. Acesso em 22.02.2024

[7] Disponível em: https://iapp.org/media/pdf/resource_center/wp216_Anonymisation-Techniques_04-2014.pdf. Acesso em 16.02.2024

[8] Disponível em: https://www.aepd.es/en/prensa-y-comunicacion/blog/anonymisation-and-pseudonymisation. Acesso em 16.02.2024

[9] Disponível em: https://www.cnil.fr/fr/lanonymisation-de-donnees-personnelles. Acesso em 22.02.2024

[10] Disponível em: https://iapp.org/media/pdf/resource_center/wp216_Anonymisation-Techniques_04-2014.pdf. Acesso em 16.02.2024

[11] Disponível em: https://ico.org.uk/media/about-the-ico/consultations/2619862/anonymisation-intro-and-first-chapter.pdf. Acesso em 16.02.2024

[12] Disponível em: https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190614%20Anonymisation%20and%20Pseudonymisation.pdf. Acesso em 16.02.2024

[13] Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em 16.02.2024

[14] Disponível em: https://ico.org.uk/media/about-the-ico/consultations/4019579/chapter-3-anonymisation-guidance.pdf. Acesso em 16.02.2024

[15] Disponível em: https://edpb.europa.eu/sme-data-protection-guide/secure-personal-data_en#:~:text=Pseudonymisation%20is%20the%20processing%20of,to%20technical%20and%20organisational%20measures.. Acesso em 16.02.2024

[16] Disponível em: https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190614%20Anonymisation%20and%20Pseudonymisation.pdf. Acesso em 16.02.2024

[17] Disponível em: https://www.cnil.fr/fr/lanonymisation-de-donnees-personnelles. Acesso em 22.02.2024

[18] Disponível em: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation_v1-(250118).pdf. Acesso em 27.02.2024

[19] Disponível em: https://ico.org.uk/media/about-the-ico/consultations/4019579/chapter-3-anonymisation-guidance.pdf. Acesso em 16.02.2024

[20] Disponível em: https://www.cnil.fr/fr/lanonymisation-de-donnees-personnelles. Acesso em 22.02.2024

Considerações TIM - Estudo Preliminar sobre Anonimização e pseudonimização para proteção de dados

1. DA ANONIMIZAÇÃO DE DADOS NA LGPD

Com relação ao parágrafo 18 do Guia de Anonimização e Pseudonimização para a Proteção de Dados Pessoais, sugerimos a alteração do texto para "Os dados anonimizados não são considerados dados pessoais, por isso não estão sujeitos à proteção da LGPD, salvo quando o processo de anonimização a que foram submetidos for revertido, utilizando exclusivamente meios próprios do agente de tratamento que o anonimizou, ou quando, com esforços razoáveis, puder ser revertido.

A sugestão consiste no acréscimo do trecho "do agente de tratamento que o anonimizou" e se justifica para evitar interpretações divergentes, com relação à possibilidade de reversão do processo por outros agentes de tratamento que não aquele que realizou a anonimização. Ainda que alguns processos de anonimização possam, teoricamente, ser revertidos, entendemos que o agente que realizou a anonimização não pode prever quando isso pode ocorrer.

2. DADOS ANONIMIZADOS E TRATAMENTO POSTERIOR/USO SECUNDÁRIO

O item 35 do Guia proposto, dispõe o seguinte: "Entretanto, se a finalidade de anonimização não houver sido informada originalmente, a sua realização importará "tratamento posterior" ou uso secundário, que, necessariamente, deverá ser compatível com a finalidade inicialmente informada aos titulares dos dados."

No caso, em se tratando de dados anonimizados que, em conformidade com o art. 12 da LGPD, não são considerados dados pessoais, não há que se falar em tratamento posterior, uso secundário ou tratamento compatível com a finalidade, uma vez que os dados submetidos o processo de anonimização não estão mais sob a égide da LGPD.

Por este motivo, entendemos pela exclusão do item mencionado.

3. DADOS ANONIMIZADOS E TRATAMENTO COMPATÍVEL COM AS FINALIDADES

O parágrafo 54 estabelece que "os dados que tenham sido tornados irreversivelmente anonimizados deixam de ser considerados 'dados pessoais' e o processamento desses dados não exige conformidade com a legislação de proteção de dados. Isso implica que as organizações podem utilizá-los para finalidades, desde que compatíveis, que vão além daquelas para as quais foram originalmente coletados e esses dados podem ser mantidos indefinidamente".

Sobre esse parágrafo, e considerando que a própria LGPD menciona, no art. 12º, que os dados anonimizados não serão considerados dados pessoais, entendemos que não deve ser exigido que o tratamento do dado tornado anonimizado ocorra para uma finalidade compatível, uma vez que os dados

submetidos a este processo não seriam, por sua natureza, protegidos pela LGPD, podendo ser utilizados livremente pelas organizações.

Nesse sentido, sugerimos a exclusão do trecho “desde que compatíveis” do parágrafo 54.

4. DA ANONIMIZAÇÃO TOTALMENTE AUTOMATIZADA

O Item “k” do apêndice, afirma que “A anonimização não deve ser totalmente automatizada - ferramentas automatizadas podem ser usadas durante o processo de anonimização, no entanto, dada a importância do contexto e a avaliação geral do processo, poderá ser necessária a intervenção de um especialista humano”.

Entendemos que sobre este tema, não é recomendável estabelecer uma proibição da anonimização de forma totalmente automatizada, objetivando, inclusive, evitar a vedação da utilização de ferramentas com considerada relevância para realização do processo, e que se valem de técnicas apuradas e seguras, que podem vir a otimizar os procedimentos, bem como gerar economia financeira e temporal para as organizações.

Desta forma, entendemos um processo de anonimização totalmente anonimizado não deva ser proibido, desde que neste sejam consideradas as melhores técnicas de segurança aplicáveis e disponíveis.

5. TÉCNICAS PARA ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO DE DADOS

O Apêndice II aborda sugestões de técnicas de anonimização e pseudonimização, objetivando elucidar em quais cenários, contextos e para qual formato de dado cada técnica abordada se mostra mais adequada.

Entendemos importante a inclusão da técnica de anonimização PCA (Principal Component Analysis), sendo esta uma técnica estatística utilizada para a redução de dimensionalidade dos dados, preservando ao mesmo tempo a maior parte da informação original. Esta técnica não só protege a privacidade, mas também oferece benefícios analíticos e econômicos significativos para as organizações.

Nesse sentido, a técnica pode ser utilizada para transformar os dados originalmente coletados em um novo conjunto de variáveis (componentes principais) que são independentes entre si.

No contexto de telefonia móvel, por exemplo, o PCA pode ser eficaz na anonimização dos dados relacionados a tráfego de dados, padrões de fidelização, geolocalização e avaliação de risco de crédito dos clientes.

Contribuições Conexis Brasil Digital - Sindicato Nacional das Empresas de Telefonia e de Serviço Móvel, Celular e Pessoal

Assunto: Consulta à Sociedade ANPD - Estudo Preliminar sobre Anonimização e Pseudonimização para Proteção de Dados

O estudo técnico em questão, conforme dispõe o presente material disponibilizado pela ANPD, visa compreender os fundamentos jurídico-normativos do processo de anonimização de dados na sistemática da LGPD no ordenamento jurídico brasileiro. Para tanto, é imprescindível que alguns pontos sejam devidamente destacados.

1. ANONIMIZAÇÃO

1.1. Da Anonimização de Dados na LGPD

Com relação ao parágrafo 18 do Guia de Anonimização e Pseudonimização para a Proteção de Dados Pessoais, sugerimos a alteração do texto para "Os dados anonimizados não são considerados dados pessoais, por isso não estão sujeitos à proteção da LGPD, salvo quando o processo de anonimização a que foram submetidos for revertido, utilizando exclusivamente meios próprios do agente de tratamento que o anonimizou, ou quando, com esforços razoáveis, puder ser revertido.

A sugestão consiste no acréscimo do trecho "do agente de tratamento que o anonimizou" e se justifica para evitar interpretações divergentes, com relação à possibilidade de reversão do processo por outros agentes de tratamento que não

aquele que realizou a anonimização. Ainda que alguns processos de anonimização possam, teoricamente, ser revertidos, entendemos que o agente que realizou a anonimização não pode prever quando isso pode ocorrer.

1.2. "Tratamento posterior" ou uso secundário da anonimização

De acordo com o indicado pela ANPD no item 35 do Estudo Preliminar, caso a finalidade de anonimização não tenha sido informada originalmente, a sua realização importará "tratamento posterior" ou uso secundário, que, necessariamente, deverá ser compatível com a finalidade inicialmente informada.

Com relação ao acima disposto, entendemos que a determinação de que o tratamento dos dados anonimizados importará em "finalidade secundária" suscita melhor esclarecimento por esta Autoridade. Pois, partindo-se do princípio de que o dado anonimizado não é considerado dado pessoal, ocorreria a exclusão da incidência da LGPD, e não haveria que se falar em finalidade secundária em seu tratamento.

Ou seja, depois que os dados pessoais forem totalmente anonimizados, não serão considerados mais dados pessoais e os usos subsequentes dos dados não serão mais regulamentados pela LGPD, a qual dispõe em seus artigos 5º, I e XI e 12º que, salvo exceções, os dados anonimizados perdem a possibilidade de associação direta ou indireta do indivíduo e, portanto, não são considerados dados pessoais.

1.3. Da gestão do risco de reidentificação

Considerando a possibilidade de reidentificação de titulares decorrentes do processo de anonimização, o guia propõe uma metodologia para gestão de riscos consistente em 4 etapas, alinhada à metodologia *risk-based approach*, que considera diversos cálculos matemáticos para determinar o risco de reidentificação.

Apesar de os agentes de tratamento precisarem ter condições de demonstrar que as técnicas de anonimização aplicadas consideram os meios próprios e esforços razoáveis disponíveis à época, a exigência de um processo como o proposto pode implicar no dispêndio de recursos (como contratação de consultorias para elaboração dos cálculos, dificultando, senão inviabilizando, a adoção de uma medida que, em última instância, tende a beneficiar os titulares de dados).

Nesse sentido, entendemos que, se de um lado, cabe à autoridade estabelecer as balizas legais, do outro, cabe aos agentes de tratamento garantir os mecanismos de governança conforme suas diretrizes internas, em razão do princípio de prestação de contas.

Dessa maneira, caso a ANPD queira auxiliar os agentes de tratamento na condução do tema, poderia sugerir a adoção de modelos mais exequíveis, a exemplo (i) das autoridades europeias, tais como a ICO, que, em seu guia de anonimização1, dispõe sobre os critérios que devem ser considerados pelas organizações sem definir uma metodologia de avaliação de risco específica, recomendando, em seu lugar, a elaboração de avaliações de impacto conforme orientações já existentes, e (ii) do método *procedure-based approach*, através da qual os agentes de tratamentos documentam os procedimentos adequados para anonimização com base nos riscos detectados previamente, que podem ser definidos com base em metodologias já praticadas pelas empresas em contextos como relatórios de impacto à proteção de dados ou testes de legítimo interesse, considerando os critérios objetivos (custo x tempo) e subjetivos (meios próprios) estabelecidos pela lei.

Ainda que a ANPD entenda relevante a recomendação da metodologia sugerida, entendemos que o guia deva, ao menos, ser revisto para melhor esclarecer como as organizações devem proceder em cada uma das etapas, incluindo o maior número possível de exemplos práticos para subsidiar os agentes de tratamento.

[1] https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf

Isto é, necessário que haja uma melhor definição do modelo de gestão de riscos que deverá ser aplicado, quais os critérios que devem ser considerados, como também os parâmetros para mensuração e tratamento desse risco, o qual não pode ser considerado como tarefa trivial, pois requer base histórica, conhecimento estatístico e competências especiais para avaliação.

Com relação ao processo de gestão de riscos de reidentificação, partindo-se do princípio de que uma efetiva anonimização no presente não afasta completamente os riscos de reversão da anonimização no futuro, nosso entendimento é de que a ANPD necessita esclarecer que, caso haja a constatação de que as condições que antes atestavam a anonimização não estejam sendo mais atendidas, tal fato não pressupõe um tratamento ilícito por parte do controlador.

Neste caso, cabe esclarecer ao controlador quais ações deverão ser tomadas, sejam elas o reinício do processo de anonimização ou a exclusão dos dados, como também quais as consequências jurídicas quando a reidentificação ocorrer por ato de terceiros.

Além disso, entendemos pela necessidade de esclarecimento quanto à eventual constatação de que as condições que antes atestavam a anonimização não estejam sendo mais atendidas, tal fato não irá pressupor um tratamento ilícito por parte do controlador.

Em conclusão, outro ponto que deve ser melhor explorado é se o modelo de avaliação de riscos envolve a condução de avaliações de impacto à proteção de dados 3 para cada processo de anonimização, já que fora indicado o dever de avaliação contínua e iterativa.

1.4. Da possibilidade de reversão do processo de anonimização. Conceito e utilização exclusiva de "meios próprios"

Nas páginas 13 e 14 do Estudo Técnico, menciona que “meios próprios” constante no Art. 12 da LGPD, de acordo com o considerando n. 26 da revogada diretiva europeia e do vigente Regulamento Geral de Proteção de Dados da UE, são tratados como meios suscetíveis de serem utilizados para (re)identificação de titular de dados aqueles adotados “seja pelo responsável pelo tratamento, seja por qualquer outra pessoa”.

Ocorre que, conforme constante na própria minuta sobre o presente tema, no item 52, temos o seguinte: “Diferentemente da noção de ‘esforços razoáveis’, o conceito de meios próprios tem conteúdo mais delimitado, podendo-se afirmar que são meios próprios as habilidades, os dados, instrumentos e técnicas disponíveis ao próprio agente de tratamento responsável pela anonimização”.

Primeiramente, da leitura acima, pode-se interpretar que a noção de “meios próprios” poderia abranger qualquer outra pessoa ou entidade que, com meios e esforços razoáveis, poderiam reidentificar o conjunto de dados anonimizados. No entanto, a expressão “meios próprios” trata-se de um critério subjetivo, diferentemente da noção de esforços razoáveis, que considera fatores objetivos como tempo, custo e tecnologia disponível. Em sendo subjetiva, tal avaliação não pretende abranger os meios disponíveis no mercado, senão os meios do próprio agente de tratamento, por isso, inclusive, o art. 12 utiliza o adverbio “exclusivamente”.

Ainda que a LGPD tenha sido inspirada no ordenamento jurídico Europeu (GDPR), é importante destacar que não é uma cópia da legislação europeia, devendo a interpretação ser realizada com a maior proximidade do que dispõe no próprio texto da Lei. Assim, a interpretação que mais se aproxima da realidade trazida pelo legislador na LGPD é a de que o uso de meios próprios será considerado os utilizados pelo próprio agente de tratamento responsável pela anonimização.

Essa definição é extremamente importante para que não ocorra qualquer responsabilização do agente de tratamento que realizou a transferência dessas informações anonimizadas para o terceiro, sem que houvesse uma observação ao

processo de governança em privacidade e proteção de dados pessoais, uma vez que, teoricamente, não há o que se falar em aplicabilidade da Lei Geral de Proteção de Dados aos dados pessoais anonimizados, no qual deixam de ser dados pessoais e passam a integrar apenas à cadeia de dados.

1.5. Proibição de anonimização inteiramente automatizada

Dispõe o item "K" do Apêndice I: "A anonimização não deve ser totalmente automatizada - ferramentas automatizadas podem ser usadas durante o processo de anonimização, no entanto, dada a importância do contexto e a avaliação geral do processo, poderá ser necessária a intervenção de um especialista humano". Nesse viés, é certo que o envolvimento humano em processos de anonimização pode ser uma medida a ser recomendada para as organizações, todavia, inexiste na LGPD qualquer proibição de que o processo de anonimização seja automatizado.

Senão por isso, com o desenvolvimento tecnológico, podem surgir ferramentas que realizam a anonimização automatizada, o que deve ser visto como algo positivo, já que permitiria a economia de tempo e recursos pelas empresas.

A limitação acima, portanto, é desarrazoada e contraria o fundamento da LGPD de desenvolvimento tecnológico, além de estabelecer uma proibição sem qualquer respaldo legal. Por esse motivo, entendemos que o item deva ser excluído do apêndice, ou, quando muito, reescrito para deixar claro que se trata de uma simples recomendação, e não de uma vedação.

2. PSEUDONIMIZAÇÃO

2.1. Da metodologia de Pseudonimização

Ao abordar sobre os requisitos para uma pseudonimização adequada, o guia da ANPD estabelece alguns passos a serem seguidos pelas organizações, incluindo a elaboração de políticas, proteção de chaves, realização de auditorias etc.

Dentre as medidas recomendadas, constam: (i) 10. Avaliação de Impacto à Proteção de Dados: realize a avaliação de impacto sobre a proteção de dados, elaborando o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) quando apropriado, a fim de avaliar os riscos associados à pseudonimização e garantir a conformidade com a LGPD. Considere a elaboração do RIPD sempre que o tratamento envolver alto risco; (ii) 11. Comunicação com os Titulares: esteja preparado para informar de forma transparente e acessível aos titulares sobre a pseudonimização e os direitos de acesso e correção de suas informações pessoais, conforme exigido pela LGPD e (iii) 12. Plano de resposta a Incidentes de Segurança: desenvolva um plano de resposta a incidentes de segurança com dados pessoais que inclua procedimentos para lidar, entre outras situações, com acessos não autorizados e tratamentos inadequados ou ilícitos, incluindo as ações de mitigação apropriadas para reverter ou mitigar os efeitos dos prejuízos gerados.

As medidas acima destacadas tratam-se, na verdade, de ações inerentes ao programa de governança dos agentes de tratamento, não tendo relação direta com o tema pseudonimização. A elaboração de um Relatório de Impacto à Proteção de Dados, por exemplo, é deflagrada conforme a atividade de tratamento que justifica a utilização do dado pessoal, não em razão do processo de pseudonimização. Vale ressaltar que a pseudonimização é, sobretudo, uma medida de segurança cujo objetivo é dificultar a identificação do titular, não se tratando de um fim em si mesmo.

Diferentemente do conceito de anonimização, portanto, que exige uma avaliação de risco para considerar a probabilidade de reidentificação do titular, não há que se falar em risco de pseudonimização, já que a atividade de tratamento anterior ao processo de pseudonimização é o que deve deflagrar ou não a avaliação de impacto.

Da mesma forma, a exigência de um plano de resposta a incidentes de segurança ou um canal para exercício de direitos dos titulares são responsabilidades inerentes de qualquer agente de tratamento, independentemente se são tratados dados pseudonimizados ou não.

Especificamente, em relação à comunicação com os titulares, salvo melhor juízo, não identificamos qual seria a utilidade de comunicá-los sobre os processos de pseudonimização da empresa. Entendemos que, como medida de segurança, tal informação deva constar em avisos de privacidade, todavia, não há necessidade de acionamento do titular para informar que, em determinada atividade, a empresa procedeu com a pseudonimização dos dados, até porque essa não é a conduta adotada para outras medidas de segurança.

Nesse contexto, entendemos que os itens 10, 11 e 12 devam ser excluídos por não haver relação direta com a atividade de pseudonimização.

Rio de Janeiro, 28 de fevereiro de 2024
OFÍCIO PRESI-033/2024

Ao Senhor
WALDEMAR GONÇALVES ORTUNHO JÚNIOR
Diretor-Presidente da
Autoridade Nacional de Proteção de Dados - ANPD

Ref.: Consulta à Sociedade acerca do Estudo Preliminar sobre Anonimização e Pseudonimização para a proteção de dados pessoais

Prezado Senhor,

A **Confederação Nacional das Seguradoras - CNseg**, entidade associativa que congrega as Federações que representam as empresas integrantes dos segmentos de seguros, resseguros, previdência privada e vida, saúde suplementar e capitalização, vem apresentar as suas contribuições à **Consulta à Sociedade acerca do Estudo Preliminar sobre Anonimização e Pseudonimização para a proteção de dados pessoais**, conforme descrito abaixo.

1. Anonimização e os princípios de proteção de dados pessoais

O Estudo divulgado pela Autoridade Nacional de Proteção de Dados - ANPD adota o entendimento de que "o ato inicial do processo de anonimização configura operação de tratamento de dado pessoal, atraindo, assim, a aplicação de princípios e regras da LGPD".

Entretanto, como a anonimização não é uma finalidade por si só, **não deveria ser considerada como atividade de tratamento de dado pessoal**. Uma vez que o artigo 16 da LGPD assegura a possibilidade de anonimização do dado **após o término do tratamento,** a anonimização não seria, então, ela própria, uma atividade de tratamento, pois ocorreria, segundo o expresso texto legal, **em um momento posterior**.

A anonimização é uma faculdade que a LGPD confere ao controlador para conservar o dado, em vez de eliminá-lo, ou, ainda, pode decorrer da decisão do controlador de minimizar os dados pessoais tratados, de modo a utilizá-los, por exemplo, apenas como base estatística - algo extremamente relevante para o mercado supervisionado pela Susep, inclusive para o aprimoramento dos cálculos que materializam os seus produtos.

Desta forma, mostra-se impertinente a sugestão do estudo para que a anonimização seja realizada em consonância com os propósitos iniciais para os quais os dados foram coletados. Os dados pessoais devem ser coletados para propósitos legítimos e informados ao titular e devem ser tratados conforme essas premissas. Porém, se após a anonimização os dados pessoais perdem a característica da identificabilidade, esses dados anonimizados não atrairiam a aplicabilidade da LGPD e, portanto, a finalidade inicial da coleta não deveria restringir o destino que o controlador dá ao conjunto formado por tais dados.

GABINETE Gustavo Brígido
Confederação Nacional das Empresas de Seguros Gerais, Previdência Privada e Vida, Saúde Suplementar e Capitalização
Rio de Janeiro - Rua Senador Dantas, 74, 16º andar | Centro | CEP 20031-205 | Tel. 21 2510 7777
www.cnseg.org.br

Aplicar os princípios da finalidade, adequação e necessidade ao processo de anonimização dos dados, tal como sugere o estudo, seria o mesmo que projetar para o tratamento de dados anonimizados as mesmas normas que incidem no tratamento de dados pessoais, contrariando a lógica da própria conclusão do estudo no sentido de que **"[d]ados anonimizados não são considerados dados pessoais, por isso não estão sujeitos à proteção da LGPD"**.

Desta forma, entende-se que o estudo deveria aclarar que **a anonimização não é uma atividade de tratamento do dado pessoal e não está submetida aos princípios e regras estabelecidos pela LGPD, que não limita os usos que poderão ser feitos com os dados anonimizados**.

2. As noções de "esforços razoáveis" e "meios próprios"

Segundo o Estudo, "a partir do texto normativo do art. 12, *caput*, da LGPD, compreende-se que a avaliação da possibilidade de reidentificação de dados e a reversão do processo de anonimização devem ter em consideração não apenas o uso de meios próprios do agente de tratamento responsável pela anonimização, mas também a atuação de outras pessoas ou entidades que, com meios e esforços razoáveis, podem reidentificar conjunto de dados anonimizados".

Esse entendimento deveria ser reavaliado. Na análise da identificabilidade do dado devem ser levados em consideração **apenas os meios detidos pelo próprio controlador, e não por terceiros**. A realização dessa análise a partir de critérios amplos e abstratos, que levem em consideração os meios também detidos por terceiros, praticamente excluiria a possibilidade de existir um dado anonimizado.

Afigura-se excessivo exigir do controlador que considere todos os meios que possam ser detidos por terceiros para avaliar a possibilidade de identificabilidade do dado. Para o setor de seguros em particular, essa tarefa seria operacionalmente impossível de ser cumprida e impactaria significativamente suas atividades, **razão pela qual se opõe à interpretação sugerida no Estudo**.

3. Gestão do risco de reidentificação

É correta a ideia de que no processo de anonimização deve ser buscada a minimização (e não a eliminação) dos riscos de reideintificação, ao mesmo tempo em que seja assegurada a manutenção da utilidade dos dados. Além disso, também parece correta a compreensão de que a gestão dos riscos de reidentificação deve ser contínua. Contudo, com relação ao que deve ser considerado para determinar o "Risco de Reidentificação Aceitável - RRA" e o "Risco de Reidentificação Mensurado - RRM", entende-se que as explicações do estudo deveriam ser simplificadas.

Para conferir maior segurança jurídica para os agentes de tratamento, sugere-se que a ANPD apresente diretrizes mais concretas e específicas de como devem ser mensurados o RRA e o RRM.

4. O Processo de Pseudonimização

O Estudo indica que "desenvolver uma metodologia eficaz de pseudonimização de dados pessoais, alinhada com as melhores práticas de mercado e em conformidade com os princípios da LGPD é fundamental para garantir a privacidade e a segurança das informações pessoais".

GABINETE Gustavo Bruno

Confederação Nacional das Empresas de Seguros Gerais, Previdência Privada e Vida, Saúde Suplementar e Capitalização
Rio de Janeiro - Rua Senador Dantas, 74, 16º andar | Centro | CEP 20031-205 | Tel. 21 2510 7777
www.cnseg.org.br

E para desenvolver uma metodologia eficaz de pseudonimização, o Estudo indica que **"devem"** ser seguidas as seguintes etapas: i) avaliação inicial e identificação dos dados objeto da pseudonimização; ii) definição de objetivos da pseudonimização; iii) seleção de técnicas de pseudonimização; iv) desenvolvimento de políticas e procedimentos; v) implementação da pseudonimização; vi) proteção das chaves e algoritmos; vii) monitoramento e auditoria; viii) treinamento e conscientização; ix) registro e documentação; x) avaliação de impacto à proteção de dados; xi) comunicação com os titulares e xii) plano de resposta a incidentes de segurança.

Entretanto, o Estudo não deveria indicar uma metodologia única para a realização da pseudonimização. **O mais adequado é deixar que o controlador, de acordo com a realidade do tratamento que é realizado, faça a avaliação da metodologia mais adequada para o processo de pseudonimização.**

As etapas sugeridas pelo estudo devem possuir viés orientativo e não taxativo, devendo ser consideradas como melhores práticas, cabendo sempre ao controlador, que é o responsável pelo tratamento, a decisão quanto à metodologia mais apropriada no processo de pseudonimização.

Colocando-se à disposição para eventuais esclarecimentos adicionais, a CNseg apresenta os protestos de consideração e respeito.

Atenciosamente,

Dyogo Oliveira
Diretor-Presidente

Confederação Nacional das Empresas de Seguros Gerais, Previdência Privada e Vida, Saúde Suplementar e Capitalização
Rio de Janeiro - Rua Senador Dantas, 74, 16º andar | Centro | CEP 20031-205 | Tel. 21 2510 7777
www.cnseg.org.br

São Paulo, 13 de março de 2024.
À Autoridade Nacional de Proteção de Dados (ANPD)

Comentários ao Estudo Preliminar sobre Anonimização e Pseudonimização para a proteção de dados pessoais

1. Sobre a MID

A associação Movimento Inovação Digital ("MID") reúne mais de 140 membros dentre plataformas digitais, meios de pagamento, empresas de investimento e demais organizações e empresas atuantes no ecossistema digital, com forte emprego da inteligência artificial em suas atividades regulares.

Dada a natureza das atividades dos membros associados e o impacto que o estudo sobre a anonimização pode ter nelas, a MID reafirma seu entendimento sobre a importância do debate relacionado com o tema. Nesse contexto, a MID reconhece os esforços empregados até o momento para debate em torno do tema.

Posto que o Estudo Preliminar impactará diretamente nas atividades de diversos atores da sociedade – incluindo-se empresas representadas pela MID – tendemos apresentar as seguintes considerações a fim de apoiar a tomada de decisão desse nobre colegiado.

2. Comentários ao Estudo Preliminar

Antes da realização dos comentários pretendidos, é preciso salutar o esforço da Autoridade Nacional de Proteção de Dados ("ANPD" ou "Autoridade") em fornecer subsídios para a correta interpretação e aplicação da Lei Geral de Proteção de Dados Pessoais ("LGPD"). Sendo a LGPD composta por uma variedade de normas principiológicas e/ou dotadas de conceitos indeterminados, faz-se necessária a atuação prevista em seu art. 55, VII, qual seja, a promoção de estudos sobre práticas nacionais e internacionais de proteção de dados.

Neste sentido, é louvável o trabalho da ANPD com relação à anonimização, tema de extrema relevância tanto para os titulares quanto para os agentes de tratamento de dados pessoais. Ademais, a decisão da ANPD de submeter o Estudo Preliminar à apreciação do público é bem-vinda, permitindo que a sociedade civil e os setores do mercado forneçam suas interpretações e contribuições sobre o tema.

O Estudo Preliminar foi embasado em três documentos, contendo: (i) análise jurídica; (ii) análise técnica e (iii) estudos de caso. Desse modo, a MID buscou contribuir em relação aos principais pontos abordados pela ANPD nas análises jurídica e técnica:

Escopo jurídico

Estudo Preliminar	Comentários MID
1. Anonimização como atividade de tratamento de dados com uma finalidade em si mesmo: a Autoridade entende que a anonimização deve possuir uma origem lícita, não possuindo a capacidade de tornar lícito um tratamento prévio. Nesse contexto, a anonimização é considerada uma operação de tratamento de dados pessoais, já que seu processo inicial depende do uso de uma base de dados.	É inequívoco que todas as atividades de tratamento de dados anteriores ao momento de anonimização são contempladas pela definição de "tratamento" e devem respeitar às regras da LGPD. Contudo, o processo de anonimização ocorre para: (1) eliminar os dados que não são necessários, considerados excessivos, em cumprimento ao princípio da necessidade e adequação; e/ou (2) para aumentar a proteção do indivíduo cujos dados estão envolvidos em uma atividade de tratamento. Isto significa dizer que o objetivo principal da anonimização não consiste em tratar um dado pessoal, para atingir uma finalidade autônoma, mas tão somente para proteger os dados pessoais, como medidas de segurança e conformidade. Além disso, considerar a anonimização como atividade de tratamento parece-nos um equívoco conceitual, em desacordo com o pretendido pelo legislador, ao editar a LGPD, pelos seguintes motivos: a) o artigo 5º, inciso XI define anonimização como o processo de 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. Ou seja, a própria lei

	define a anonimização como a aplicação de medidas de proteção para desidentificação dos titulares de dados no momento do tratamento de dados, e não como uma atividade de tratamento em si; b) o legislador optou por listar, como exemplo, 20 condutas que representem atividades de tratamento (art. 5º, X), e em outro dispositivo trouxe o conceito de anonimização (art. 5º, XI)"; c) mesmo fora do rol do artigo art. 5º, X, o legislador deixou expresso que a atividade de pseudonimização era uma atividade de tratamento (vide redação do art. 13, § 4º), o que não aconteceu com a anonimização. d) a LGPD recomenda a anonimização como uma prática em certos contextos, como em estudos por órgão de pesquisa (arts. 7º, IV e 11, II, "c"), estudos em saúde pública (art. 13), mas não a estabelece como uma obrigação legal para o tratamento de dados. e) anonimização também foi considerada no artigo 18, IV, como um direito que o titular de dados pode requerer para proteger seus dados de um tratamento excessivo, desnecessário ou em desconformidade com a LGPD. Esse conjunto de normas sugere que a anonimização é uma medida de proteção adicional recomendada, não uma atividade de tratamento de dados em si, exigida pela legislação; e

	f) o artigo 12 da LGPD estabelece que os dados anonimizados deixam de ser considerados dados pessoais. Isso reflete o entendimento de que a anonimização serve para reduzir o risco e a responsabilidade associados ao tratamento de dados pessoais, e não um processo de tratamento autônomo com uma finalidade própria. Desta maneira, entende-se que a anonimização não deveria ser considerada como uma operação de tratamento autônoma, mas como uma medida técnica acessória destinada a garantir a conformidade e segurança de uma base de dados. Portanto, recomendamos que a Autoridade reveja o posicionamento ao classificar a anonimização como uma atividade de tratamento de dados pessoais autônoma.
2. Aplicação dos princípios da LGPD no processo de Anonimização: Com a premissa de que a anonimização é uma atividade de tratamento com uma finalidade em si mesma, a ANPD entende que seria necessário observar os princípios previstos pelo art. 6º da LGPD. Além disso, o agente de tratamento deveria atribuir uma base legal e informar aos titulares que pretende realizar a anonimização (finalidade), que deverá ser compatível com a finalidade originária (adequação) e utilizada para minimizar a	Considerar a anonimização como uma operação autônoma de tratamento de dados impõe obrigações adicionais ao processo de anonimização, o que pode dificultar a utilização dessa medida de segurança e conformidade na prática. Sobre base legal: se anonimização vier a ser considerada uma atividade de tratamento, o controlador deverá observar: ● Princípio da legalidade e, portanto, atribuir uma

quantidade de dados tratados (necessidade), para realizar a anonimização de forma lícita.	base legal para a ação de anonimização. Entretanto, como exposto no item 1 acima, a anonimização não tem finalidade própria, mas tem como objetivo garantir conformidade do tratamento e a proteção do dado pessoal. Por este motivo, a ANPD deveria rever seu posicionamento na minuta do Guia sob consulta, para que a base legal atribuída à finalidade originária/primária fosse suficiente para aplicação das ferramentas e processos de anonimização; • Princípio da adequação: a Autoridade pretende que a anonimização seja adequada ao tratamento anteriormente realizado. Contudo, a realização da anonimização pressupõe que o conjunto de dados anteriormente tratado perderá o caráter de dado pessoal, não havendo como verificar se o tratamento posterior é ou não adequado às finalidades informadas ao titular. • Princípio da transparência (1): A proposta do Guia parece exigir que o controlador informe ao titular se há técnica que pode limitar o uso dos dados para o propósito original. Essa obrigação deve ser relativizada, pois o controlador pode não saber, durante o tratamento, se os objetivos definidos quando os dados foram coletados podem ser

	alcançados se os dados forem anonimizados; • Princípio da transparência (2): o Estudo menciona brevemente a necessidade de que os agentes de tratamento se comuniquem de forma transparente com os titulares sobre os processos de pseudonimização. No entanto, não há detalhamento sobre quais informações devem ser repassadas ao titular. Nesse ponto, a ANPD deveria detalhar quais informações específicas mínimas devem ser comunicadas ao titular de dados para garantir a transparência do processo de pseudonimização; Finalmente, a forma pela qual a anonimização é tratada no Estudo Preliminar não deixa claro se efetivamente esta operação representa a extinção do tratamento de dados pessoais, especialmente considerando a ausência de menções a este tema nos documentos disponibilizados. Em paralelo, na Tomada de Subsídios sobre os direitos dos titulares, a ANPD reservou uma seção para discutir o embate entre a eliminação dos dados e a anonimização para atender aos direitos dos titulares, o que não foi feito no Estudo Preliminar e nos parece tornar a discussão sobre este tema incompleta. Sugere-se, portanto, unificar o entendimento em ambos os instrumentos, compatibilizando as diretrizes neles contidas, ainda que de forma remissiva.

3. Aplicabilidade de conceitos determinantes (1): O estudo da ANPD busca parâmetros para definir os “meios suscetíveis de ser razoavelmente utilizados”, “esforços razoáveis” e “meios próprios”. A ANPD propõe que o conceito de “meios razoáveis”, é dinâmico e contextual, devendo ser analisado de acordo com os meios disponíveis para a reidentificação de dados pessoais em um momento específico, com base em critérios como tempo, custos, estado da arte, técnicas de reidentificação. Nesse contexto, a ANPD admite que a anonimização é uma atividade de risco e, portanto, de resultado incerto. Isso demanda que o controlador adote ações para medir e avaliar os riscos de reidentificação.	A proposta do Guia destaca a importância de considerar fatores como custo, tempo e tecnologias disponíveis na avaliação da viabilidade da reidentificação de dados, para então identificar o que é de “esforços razoáveis” e “meios próprios” para reidentificação de dados. No entanto, a falta de parâmetros específicos para definição desses conceitos (custos razoáveis, duração aceitável e tecnologias disponíveis) gera incertezas e dificuldades na aplicação prática desses critérios. Nossa sugestão, consiste na complementação do guia sobre dois aspectos: ● maior detalhamento dos fatores que devem ser considerados para determinação do risco de identificação; ● detalhar quais são as responsabilidades dos controladores e operadores no processo de anonimização; ● fornecer exemplos práticos que auxiliem os agentes de tratamento a interpretar e determinar seus próprios limites. Sobre a responsabilidade dos agentes de tratamento, é importante que a ANPD distinga a responsabilidade do agente que realiza a anonimização daqueles agentes que consomem a base de dados após o processo de anonimização. Por exemplo, enquanto o agente

	anonimizador deveria responder pelos requisitos estabelecidos no Estudo Preliminar, os agentes que utilizam a base supostamente anonimizada poderiam ser isentos de responsabilidade, já que não possuem controle sobre o processo de gestão de riscos de reidentificação. Sobre o detalhamento dos fatores, o Guia poderia explorar, por exemplo, os seguintes critérios: ● tamanho/volume do conjunto de dados; ● número de registradores únicos e diretos utilizados no processo; ● nível de detalhe/granularidade da informação (p.ex: um conjunto de dados contém idades exatas dos respondentes. Anonimizar os dados para incluir apenas a faixa etária (20-30, 30-40, etc.) reduziria o risco de reidentificação; ● Diversidade/variabilidade dos atributos (p.ex. lista de empregados, quando há um cargo único dentro de uma empresa, como o CEO); ● Disponibilidade de outros dados públicos que permitam o cruzamento com os dados anonimizados; e ● Efetividade das técnicas de anonimização. Por fim, a ANPD também poderia trazer recomendações de ações a serem adotadas caso seja constatada alta possibilidade ou concretização de reidentificação de titulares de dados a partir uma base

	de dados considerada anonimizada. No caso, é importante que Guia afaste a responsabilidade dos agentes que utilizam base de dados anonimizadas, de boa-fé, e garantindo a não reidentificação no seu ambiente, caso haja falhas na anonimização realizada pelo agente de tratamento originário.

Escopo técnico	
Estudo Preliminar	**Comentários MID**
4. Aplicação do cálculo de ponderação (utilidade x anonimização): A ANPD determina que os agentes de tratamento devem se orientar por um cálculo de ponderação entre duas variáveis, quais sejam, a utilidade dos dados e o grau de anonimização destes; Nesse contexto, os controladores devem encontrar o equilíbrio ideal entre "Utilidade x Anonimização" em suas atividades, evitando que: *(i)* a anonimização excessiva comprometa a utilidade de suas informações; ou *(ii)* que a ausência de anonimização signifique a violação da lei ou a exposição de titulares;	A ANPD poderia apresentar um framework para guiar a decisão do nível de anonimização a ser aplicada, levando em conta o equilíbrio entre risco e utilidade. Ou seja, regras e parâmetros claras para diferentes situações, tipos de dados ou metas de análise, incluindo exemplos práticos. A ANPD também poderia oferecer orientações sobre como documentar e justificar as escolhas de técnicas de anonimização e pseudonimização, ajudando as organizações a atenderem o princípio da responsabilização e prestação de contas (art. 6º, X).
5. Gestão contínua de riscos: a minuta do Guia propõe uma gestão contínua dos riscos de reidentificação dos titulares.	A metodologia proposta pela minuta Guia pode ser complementada para facilitar a sua utilização pelos agentes de tratamento:

Para a gestão do risco, a Autoridade Nacional fornece metodologia específica, estabelecendo as métricas de Risco de Reidentificação Aceitável (RRA) e Risco de Reidentificação Mensurado (RRM). Os agentes deverão, antes da anonimização, estabelecer um padrão aceitável de risco (RRA), baseado em critérios variáveis, dentre os quais a ANPD traz como exemplo a presença de dados sensíveis ou dados financeiros. Após a definição do parâmetro aceitável, deve ser realizada a anonimização e mensurado o risco concreto detectado (RRM), utilizando métricas arbitrárias como nível de acesso ao dado e métricas contextuais (ex: equivalência de classe e unicidade dos dados). Detectado um risco (RRM) maior do que o aceitável (RRA), o processo será considerado insuficiente e a anonimização deverá ser realizada novamente, sob pena de não serem considerados dados anonimizados.	• os critérios propostos na metodologia não estão devidamente explicados, tampouco há parâmetros para sua medição e aplicação. Isto torna a metodologia proposta inócua, com alta probabilidade de ser pouco utilizada (vide critérios inseridos no item 3 acima) ; • também não há exemplos práticos de aplicação da fórmula, o que também pode desestimular/dificultar sua utilização correta; • A ANPD deve detalhar como a documentação tanto das etapas da anonimização quanto das etapas do processo de gestão deve ser elaborada pelos agentes de tratamento; • Indicar os relatórios de impacto à proteção de dados (“RIPD”, previstos pelo art. 5º, XVII, LGPD) como instrumento adequado para documentação da avaliação do risco de reidentificação, e, nesse sentido, sugerir modelo de relatório para essa finalidade, com exemplos práticos; • a ANPD poderia explorar aspectos práticos para realização de testes de penetração e simulações de ataques de reidentificação, utilizando as técnicas mais recentes. Isso pode incluir ataques de inferência, ataques baseados em machine learning e outros métodos de análise avançada. O objetivo é ajudar os agentes de tratamento a identificar vulnerabilidades antes que sejam exploradas por atacantes reais; e

	• a ANPD deve aproveitar a oportunidade para reforçar e estimular que os setores econômicos a se autoregularem sobre a metodologia ou variáveis do cálculo. Recomendamos uma etapa adicional e específica junto as associações e entidades representativas no próprio processo de tomada de subsídio para essa finalidade, em razão do pouco tempo para essas discussões.
6. pontos não abordados pela proposta do Guia e estudos preliminares:	Recomendamos que a ANPD aborde os seguintes temas no Guia: a) sugestões de cláusulas contratuais padrão para regulamentar o processo de anonimização e/ou compartilhamento de dados anonomizados; b) regulação específica para os agentes de pequeno porte, e os demais agentes que compartilham dados de tratamento com os agentes de porte, sobre recomendações razoáveis a serem implementados; c) orientar que as técnicas de anonimização e pseudonimização, a depender do risco de reidentificação, pode eximir o agente de tratamento dos deveres de comunicações do artigo 48 em caso de incidentes de segurança, considerando o potencial de redução do risco para os titulares de dados afetados.

3. Considerações finais

Por fim, reiteram-se os cumprimentos à Autoridade Nacional de Proteção de Dados pelo esforço na realização do presente Estudo Preliminar e pela convocação da Consulta à Sociedade. A contribuição da MID objetiva trazer subsídios e comentários no sentido de trazer o posicionamento de suas integrantes, bem como de contribuir com a construção de um entendimento sobre a anonimização que seja preciso e capaz de fornecer segurança jurídica para os agentes de tratamento e garantir os direitos dos titulares de dados.

Respeitosamente,

Comitê de Privacidade e Proteção de Dados,
Movimento Inovação Digital.
Apoio Jurídico: Opice Blum Advogados

GRUPO DE TRABALHO DE PROTEÇÃO DE DADOS - FIEMG

Gerência de Segurança da Informação e Proteção de Dados

Ref.:: Estudo Preliminar - Anonimização e pseudonimização para proteção de dados

O Sistema FIEMG, em nome do Grupo de Trabalho instituído com a finalidade de analisar as disposições legais e regulatórias sobre proteção de dados, apresenta as seguintes contribuições sobre o Estudo Preliminar - Anonimização e pseudonimização para proteção de dados.

Incialmente, considerando os fundamentos da LGPD, em especial aquele que dispõe sobre o desenvolvimento econômico e tecnológico e a inovação, a temática de anonimização e pseudoanonimização necessita de amadurecimento do mercado tecnológico, inclusive sob as perspectivas de análise do risco *versus* o valor investido.

Ao realizar a leitura do Estudo, um ponto importante de esclarecimento diz respeito ao papel da anonimização como atividade de tratamento de dados ou como mera medida técnica: é considerado, portanto, um tratamento de dado pessoal conforme elencado no rol exemplificativo do Art.5, X da LGPD, como por exemplo, “processamento”? Ou seria apenas uma ferramenta meio, tendo em vista que após aplicação efetiva da anonimização, as informações já não serão consideradas dados pessoais para os fins da LGPD?

Ainda na situação acima, sob a ótica de que os dados pessoais submetidos ao processo de anonimização devem ser, na origem, objeto de legítimo tratamento pelo agente responsável, ou seja, o tratamento de origem precisa estar fundamentado no Art.7 ou no Art.11 da LGPD, e no cenário do processo de anonimização ser considerado tratamento de dado pessoal, seria necessário fazer uma nova atribuição de base legal, distinta do tratamento originário?

Aliado ao questionamento acima, no cenário do processo de anonimização ser considerado tratamento de dado pessoal, para a conservação dos dados após o término do tratamento para uso exclusivo do controlador (art. 16, IV da LGPD), seria o cumprimento de obrigação legal ou regulatória a hipótese legal apropriada para fundamentar?

Ainda, considerando a necessidade de respeito aos princípios da finalidade e da adequação, e que os processos de anonimização e pseudoanonimização de dados podem ser realizados durante e depois do tratamento dos dados, como deve se dar a análise de compatibilidade com as finalidades que eram esperadas pelo titular?

No presente Estudo, o conceito de reindentificação resultou em dúvida quanto à diferenciação da reversão citada no Art.12 da LGPD. Isto porque o Estudo destaca que a anonimização não

reduz a probabilidade de reidentificação de um conjunto de dados a zero, isto é, a anonimização não elimina todo e qualquer risco de reidentificação. Dito isto, indagamos: seriam conceitos sinônimos? Caso positivo: A aplicabilidade do Art.12 é subjetiva e acarreta insegurança jurídica. Caso negativo: Importante conceituar o termo “reversão”.

Cabe destacar ainda, que algumas técnicas apresentadas, por exemplo Adição de Ruído e Permutação, compromete o princípio da qualidade do dado destacado no Art.6, V da LGPD. Além do mais, vai de encontro com o informado no Estudo de manter os dados anonimizados funcionais, uma vez que a leitura das bases de dados com a aplicação de tais técnicas poderá ser induzida ao erro.

Belo Horizonte, 23 de Fevereiro de 2024

UFMG
UNIVERSIDADE FEDERAL
DE MINAS GERAIS

Para: Autoridade Nacional de Proteção de Dados (ANPD)

De: Mário S. Alvim & Gabriel H. Nunes

Assunto: Consulta à Sociedade sobre a minuta do Guia de Anonimização e Pseudonimização para a Proteção de Dados Pessoais

Data: Fevereiro de 2024

Escrevemos em resposta à "Consulta à Sociedade sobre a minuta do Guia de Anonimização e Pseudonimização para a Proteção de Dados Pessoais", proposta pela Autoridade Nacional de Proteção de Dados (ANPD). Somos pesquisadores em privacidade e membros do Laboratório INSCRYPT (Laboratory of Information Security, Cryptography, Privacy, and Transparency) do Departamento de Ciência da Computação (DCC) da Universidade Federal de Minas Gerais (UFMG), responsável pelo Termo de Execução Descentralizada (TED) 8750 acordado entre o Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (INEP) e a UFMG.

Conforme a Minuta do Estudo Preliminar publicada pela ANPD, em seus itens 61, 62, e 63, estabelecer um processo contínuo de monitoramento dos riscos à privacidade, assim como considerar as especificidades de cada agente de tratamento, são observações desejáveis e necessárias à correta aplicação de métodos de controle de divulgação de dados. Entretanto, nos causa preocupação o uso de métricas de risco obsoletas e subjetivas, em desacordo com o atual consenso científico que preza por métodos matemáticos formais.

Especificamente, desconhecemos suporte teórico na literatura científica atual sobre as métricas "Risco de Reidentificação Aceitável (RRA)" e "Risco de Reidentificação Mensurado (RRM, ou Métrica Contextual)", apresentadas no documento em seus itens 64 ao 75. Dessa forma, não há clareza sobre as garantias matemáticas de que a aplicação de tais métricas ao tratamento de dados resultaria no correto e desejado controle dos riscos à privacidade dos indivíduos.

Ademais, a sugestão de uso de métodos de controle de divulgação de dados como k-Anonimização, ℓ-Diversidade, e t-Proximidade, conforme item 71 e Apêndices II, III, e IV do documento, assim como o uso de técnicas como "supressão, generalização, mascaramento, adição de ruídos e permutação", conforme Apêndices II, III, e IV do documento, está em desacordo com as melhores práticas adotadas internacionalmente e, novamente, em desacordo com o atual consenso científico. Ressaltamos aqui as alterações realizadas pelo Escritório do Censo dos Estados Unidos da América, o qual abandonou o uso de tais métodos e técnicas a partir da divulgação do Censo de 2020 devido aos severos riscos à privacidade existentes nos dados publicados mesmo após a aplicação de tais métodos e técnicas.

Finalmente, nos causam preocupação os exemplos anedóticos apresentados como "Estudo de Casos", conforme Apêndice IV do documento, os quais não correspondem às dimensões e

características de bases de dados reais. Por exemplo, os microdados dos Censos Educacionais anteriormente publicados pelo INEP abrangiam mais de 50 milhões de cidadãos brasileiros e quase uma centena de atributos. Dessa forma, um risco de re-identificação igual a 35%, como proposto no Estudo de Caso 3, com base em critérios subjetivos, corresponderia à completa re-identificação de ao menos 17,5 milhões de indivíduos e o imediato acesso às respectivas informações contidas nas dezenas de atributos disponíveis nos microdados.

Enfatizamos o atual consenso científico em torno de métodos matemáticos formais e a importância de modelos matematicamente corretos e corroborados por experimentos exaustivos quando da análise de riscos à privacidade de indivíduos. Em especial, ressaltamos a importância da "Nota de esclarecimento | Divulgação dos microdados" publicada pelo INEP em 22 de fevereiro de 2022, assim como dos Relatórios Técnicos do Termo de Execução Descentralizada (TED) 8750, no qual aplicamos o estado-da-arte para a análise de riscos à privacidade dos cidadãos brasileiros representados nos microdados dos Censos Educacionais do INEP.

Atenciosamente,

gov.br
Documento assinado digitalmente
MARIO SERGIO FERREIRA ALVIM JUNIOR
Data: 26/02/2024 20:31:40-0300
Verifique em https://validar.iti.gov.br

Mário S. Alvim
Professor
Departamento de Ciência da Computação,
Universidade Federal de Minas Gerais
ORCiD: 0000-0002-4196-7467

gov.br
Documento assinado digitalmente
GABRIEL HENRIQUE LOPES GOMES ALVES NUNI
Data: 26/02/2024 20:35:02-0300
Verifique em https://validar.iti.gov.br

Gabriel H. Nunes
Doutorando
Departamento de Ciência da Computação,
Universidade Federal de Minas Gerais
School of Computing,
Macquarie University
ORCiD: 0000-0002-7823-3061

I. INTRODUÇÃO

Respeitando a agenda regulatória do biênio 2023-2024, publicada em 04 de novembro de 2022 (Portaria ANPD n. 35), a Autoridade Nacional de Proteção de Dados disponibilizou recentemente Estudo Preliminar sobre Anonimização e Pseudonimização para a proteção de dados pessoais, estudo este que submete a contribuições da sociedade no tema. Este estudo é o resultado da junção do Estudo Técnico sobre a anonimização de dados na LGPD: análise jurídica, o Estudo Técnico sobre a anonimização de dados na LGPD: Uma visão de processo baseado em riscos e técnicas computacionais e o Estudo de casos sobre anonimização de dados na LGPD.

Trazemos abaixo, portanto, os principais pontos de atenção que, em nossa opinião, ainda merecem maiores esclarecimentos pela Autoridade, objetivando subsidiar a compreensão da associação sobre o assunto.

De forma resumida, os principais pontos de atenção da norma, em nossa visão, são:

I. DA FINALIDADE COMPATÍVEL COM O TRATAMENTO (3.1.)

PEDIDO DE ESCLARECIMENTO
Roga-se à autoridade que esclareça parâmetros claros sobre o que seria considerada finalidade compatível ou incompatível na ocasião em que a finalidade de anonimização não houver sido informada originalmente ao titular dos dados.

II. DA TECNOLOGIA DISPONÍVEL AO AGENTE DE TRATAMENTO (3.1.)

PEDIDO DE ESCLARECIMENTO
Roga-se à autoridade que forneça esclarecimentos acerca do risco de reidentificação de dados ao considerar recentes tecnologias, como sistemas de inteligência artificial. Importa que a Agência considere, ainda, que tais tecnologias, sobretudo quando a capacidade é desconhecida pelos demais agentes de mercado, devem ser consideradas elementos alheios aos termos do art. 12, não podendo se enquadrar em parâmetros de "meios próprios" ou "esforços razoáveis".

III. QUANTO A APLICABILIDADE DOS PRINCÍPIOS E DEVERES DA LGPD AO PROCESSO DE ANONIMIZAÇÃO (item 3.1.1.)

SUGESTÃO DE ADIÇÃO
Roga-se à autoridade que deixe explícito que a observância dos princípios da LGPD, bem como, da realização da avaliação descrita no parágrafo 37 do estudo, são ações a serem realizadas previamente a aplicação das técnicas de anonimização. Uma vez estas sendo bem-sucedidas, não haveria necessidade de compatibilizar as finalidades originárias de tratamento dos dados pessoais com os usos que os agentes de tratamento pretendem realizar com a base de dados anonimizada, uma vez que os dados anonimizados não estão sob o âmbito da incidência da LGPD.

IV. QUANTO AO RISCO DE REINDENTIFICAÇÃO (item 3.1.2.)

SUGESTÃO DE ADIÇÃO
Roga-se à autoridade que apresente o risco de reindendificação por meio da análise de casos que exponham técnicas mais aderentes a realidade do mercado, com exemplos que tratem de banco de dados não estruturados, e que se utilizam de técnicas sofisticadas de anonimização, como aquelas baseadas no uso de inteligência artificial.

V. QUANTO AS NOÇÕES DE ESFORÇOS RAZOÁVEIS E MEIOS PRÓPRIOS (item 3.1.3)

PEDIDO DE ESCLARECIMENTO
Comentário a ser inserido no espaço para contribuição: "Roga-se à autoridade o esclarecimento quanto aos aspectos que ela valorativamente poderá considerar para densificar o conceito de esforços razoáveis. Adicionalmente, requer-se o esclarecimento sobre a necessidade de análise de esforços de terceiros, quando o art.12 caput e §1º LGPD vincula a análise de reindentificação exclusivamente ao uso de meios próprios."

VI. QUANTO A GESTÃO DO RISCO DE REINDENTIFICAÇÃO (3.2.2.)

SUGESTÃO DE ADIÇÃO AO PARÁGRAFO 63
Este processo é apenas uma das diferentes possibilidades existentes que o agente de tratamento poderá se amparar para avaliar o risco de reindentificação de determinado processo de anonimização, inclusive, mas não se limitando a análises não probabilísticas, como as análises contextuais.

SUGESTÃO DE ADIÇÃO
Roga-se à autoridade que deixe explícito o caráter meramente orientativo e sugestivo da proposta de processo de anonimização baseada em riscos indicada no item 3.2.2, de modo a não afetar a liberdade dos agentes de tratamento em escolher a técnica, o modelo, o procedimento e o tipo documental adequado ao contexto do tratamento dos dados objeto da anonimização.

São Paulo, 14 de março de 2024

À AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS ("ANPD")
Coordenação-Geral de Normatização

A ASSOCIAÇÃO BRASILEIRA DE REDES DE FARMÁCIAS E DROGARIAS ("Abrafarma"), pessoa jurídica constituída na forma de associação civil sem fins lucrativos, com sede na Alameda Santos, 2300 - Cerqueira César, Cidade de São Paulo, Estado de São Paulo, é uma entidade de representação nacional focada no bem-estar e na saúde dos brasileiros, que reúne organizações atuantes no varejo farmacêutico.

Em 30 de janeiro de 2024, a ANPD disponibilizou, por meio da Plataforma "Participa + Brasil",[1] Consulta à Sociedade[2] acerca do seu Estudo Preliminar sobre Anonimização e Pseudonimização para Proteção de Dados ("Estudo Preliminar"), a fim de coletar contribuições de profissionais da área, agentes de tratamento, titulares, setor acadêmico e da sociedade em geral. A consulta pretende alinhar a atuação regulatória da Autoridade às melhores práticas em matéria de anonimização e pseudonimização de dados pessoais.

Nessa oportunidade, a Abrafarma vem apresentar a sua contribuição à ANPD, reiterando seus cumprimentos pela iniciativa de consultar e colher subsídios de todos os setores interessados com vistas a contribuir para a atuação da autoridade em torno do tema.

[1] "Consulta à Sociedade - Estudo Preliminar - Anonimização e pseudonimização para proteção de dados". Disponível em: <https://www.gov.br/participamaisbrasil/consulta-a-sociedade-estudo-preliminar-anonimizacao-e-pseudonimizacao-para-protecao-de-dados>. Acesso em: 13.03.2024.

[2] "ANPD abre consulta à sociedade sobre o Guia de Anonimização e Pseudonimização". Disponível em:<https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-abre-consulta-a-sociedade-sobre-o-guia-de-anonimizacao-e-pseudonimizacao>. Acesso em: 13.03.2024.

CONSULTA À SOCIEDADE SOBRE O GUIA DE ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO

- **Termos Definidos**. Inicialmente, a Abrafarma destcasa que os termos definidos pela ANPD no Estudo Preliminar (parágrafo 8) disponibilizado no âmbito desta Consulta poderiam ser indicados diretamente no Glossário de Proteção de Dados Pessoais e Privacidade recentemente publicado pela Autoridade,[3] garantindo a uniformidade do entendimento conceitual e técnico da ANPD em um único documento. O Glossário indica os principais conceitos, termos e expressões usados na Lei Geral de Proteção de Dados Pessoais (Lei Federal n.º 13.709/2018 ou "LGPD") e nos documentos da ANPD, de modo que o documento poderia reunir as informações contidas no parágrafo 8 do Estudo Preliminar.

- **Anonimização e Tratamento de Dados Pessoais**. Ao contrário do indicado pela ANPD em seu Estudo Preliminar, a anonimização de dados pessoais não é, por si só, uma atividade de tratamento, conforme definição do artigo 5º, X, da LGPD. Embora a ANPD afirme que a anonimização se inicia com o processamento de dados pessoais (parágrafo 27 do Estudo Preliminar), fato é que a anonimização não pode ser entendida como um tratamento de dados em si mesma, de modo que dependa de fundamentação em hipótese legal da LGPD. Isso porque: ***(i)*** a anonimização não contraria a finalidade inicial do tratamento realizado pelo agente de tratamento – como consagrado na experiência internacional e no Considerando 50 do Regulamento Geral sobre a Proteção de Dados 2016/679 da Europa ("GDPR"); e ***(ii)*** a necessidade de fundamentar a anonimização de dados em alguma hipótese legal poderia, em última instância, inviabilizar a utilização de dados que não mais estariam sujeitos às regras da LGPD para diferentes fins além dos previstos nas bases legais da legislação. Assim, defende-se que a anonimização seja tida como uma medida de segurança, e não como um tratamento que dependa de nova base legal e finalidade de tratamento de dados.

  Além disso, como a anonimização compreenderia uma atividade voltada à perda da associação do dado pessoal ao titular, ela estaria relacionada com as atividades de tratamento anteriores conduzidas pelo agente. Por isso, a Abrafarma considera importante que a ANPD esclareça que o processo de anonimização não depende de nova fundamentação em hipótese legal prevista no artigo 7º ou 11 da LGPD, tendo em vista a compatibilidade da operação com as finalidades originais para as quais as informações eram tratadas, consoante o GDPR, inspiração normativa para a LGPD.

---

[3] ANPD. "ANPD lança Glossário de Proteção de Dados Pessoais". Disponível em:<https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-lanca-glossario-de-protecao-de-dados-pessoais>. Acesso em: 13.03.2024.

Ademais, uma vez que a LGPD tem por objetivo proteger as liberdades e os direitos do titular, e que a anonimização fortaleceria essa proteção, a Abrafarma entende que a necessidade fundamentar o processo de anonimização em nova hipótese legal poderia inviabilizar a implementação dessa medida de segurança pelo agente de tratamento. Por esse motivo, a ANPD poderia indicar expressamente que a anonimização não corresponde a uma atividade de tratamento desassociada da finalidade inicial para a qual as informações eram operadas.

- **Princípio da finalidade**. Ao contrário do que se sugere no parágrafo 54 do Estudo Preliminar, o agente não deve, após a anonimização, garantir a aplicação dos princípios previstos na LGPD durante o uso dos dados anonimizados, haja vista que eles deixam de ser aplicáveis. Esse entendimento é, inclusive, corroborado pelo Guidance on Anonymisation and Pseudonymisation,[4] da autoridade de proteção de dados da Irlanda. A bem da verdade, o agente de tratamento é livre para operar com as informações sobre as quais a LGPD não é aplicável, inclusive para finalidades que não sejam compatíveis com o tratamento anterior. Vale destacar que dados irreversível e eficazmente anonimizados não são mais reputados como dados pessoais e os princípios de proteção de dados não precisam ser cumpridos em relação a essas informações, consoante orientação da autoridade de proteção de dados da Irlanda, de forma que o controlador poderia, por consequência, utilizar os dados anonimizados para outros fins.

- **Princípio da necessidade**. O artigo 16, IV, da LGPD, não condiciona a conservação de dados anonimizados, após o término do tratamento dos dados pessoais, à garantia do princípio da necessidade, ao contrário do indicado pela ANPD no parágrafo 39 do Estudo Preliminar. Com efeito, essa previsão parece exceder a previsão da lei, atribuindo interpretação restritiva diferente daquela prevista pelo legislador, especialmente porque os dados anonimizados não estão sujeitos à normativa consagrada pela LGPD (art. 1º c/c art. 5º, I, LGPD), incluindo seus princípios. Assim, o controlador pode operar dados anonimizados sem necessidade de limitar as suas operações ao mínimo necessário para a concretização dos seus propósitos ou de abranger somente dados pertinentes, proporcionais e não excessivos em relação às finalidades iniciais do tratamento dos dados pessoais não anonimizados (artigo 6º, III, LGPD). Isso ocorre porque, a partir da anonimização, o agente será livre para tratar as informações como quiser, razão pela qual se recomenda a exclusão da menção ao princípio da necessidade no parágrafo 39 do Estudo Preliminar.

---

[4] Data Protection Comission. "Guidance on Anonymisation and Pseudonymisation". Disponível em:<https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190614%20Anonymisation%20and%20Pseudonymisation.pdf>. Acesso em: 13.03.2024.

- **<u>Responsabilidade do controlador pela reidentificação</u>**. A possibilidade de reidentificação do titular por terceiros, sem que haja culpa do controlador, não corresponde a tratamento ilícito do controlador. Ao contrário do indicado pela ANPD no parágrafo 31 do Estudo Preliminar, o agente não teria incorrido em violação a qualquer dispositivo da LGPD pela reidentificação conduzida por terceiros, em especial porque o artigo 12 da legislação se refere a somente "meios próprios".

  Dessa forma, a Abrafarma compreende que a ANPD poderia revisar seu Estudo Preliminar para indicar que a reversão do processo de anonimização por terceiros não representaria tratamento irregular pelo agente que anonimizou inicialmente os dados. Nesse sentido, o agente não poderia ser responsabilizado pela reidentificação (artigo 43, I, LGPD), desde que esteja em conformidade com os requisitos estabelecidos pela LGPD, já que nenhum processo de anonimização é perpétuo (Apêndice I, alínea "c", do Estudo Preliminar).

  Além disso, segundo a LGPD, as técnicas de anonimização a serem utilizadas pelo agente de tratamento são aquelas "razoáveis e disponíveis no momento do tratamento" (art. 5º, XI, LGPD). Com isso, recomenda-se que a ANPD esclareça que, no evento do surgimento de uma nova tecnologia capaz de reverter o processo de anonimização anteriormente conduzido pelo agente de tratamento, este não poderá ser responsabilizado, vez que cumpriu com a exigência disposta na LGPD quando do momento em que realizou a anonimização.

- **<u>Risco de reidentificação aceitável</u>**. A definição do "risco de reidentificação aceitável" a ser estipulada pelo próprio agente de tratamento (parágrafo 65 do Estudo Preliminar) pode colidir com os entendimentos fiscalizatórios posteriores da ANPD, gerando insegurança jurídica em eventuais processos de anonimização e pseudonimização. Sugere-se que a Autoridade preveja com maior especificidade quais os parâmetros de estabelecimento desse risco, para que o agente proceda à ponderação de interpretações que observem, de um lado, a visão do agente regulado; de outro, da ANPD. A Abrafarma compreende que um maior aprofundamento da Autoridade nesse ponto auxiliaria os agentes de tratamento a identificar as melhores metodologias aplicáveis ao processo de anonimização.

- **<u>Reversão da anonimização</u>**. A razoabilidade dos esforços para a reversão do processo de anonimização (artigo 12, LGPD) não é um conceito jurídico indeterminado, como previsto no parágrafo 48 do Estudo Preliminar, uma vez que o próprio artigo 12, § 1º, da LGPD apresenta exemplos de fatores específicos que devem ser levados em consideração para a sua definição no caso concreto. Ainda assim, a ANPD pode auxiliar os agentes de tratamento na identificação e na análise dos fatores descritos no artigo 12, § 1º, da LGPD, sem contrariar o que dispõe a legislação – notadamente a limitação de que a reidentificação tem que ser possível por "meios próprios". Logo, a Abrafarma entende que a Autoridade

poderia suprimir a menção à teoria do conceito jurídico indeterminado presente no parágrafo 48 do Estudo Preliminar.

- **Uso de meios próprios na anonimização**. A LGPD indica que os dados anonimizados não serão considerados dados pessoais, salvo quando o processo de anonimização puder ser revertido, utilizando exclusivamente meios próprios (artigo 12, LGPD). Por isso, não seria possível à ANPD sustentar que o processo de anonimização pode ser revertido a partir de meios de terceiros, como prevê o parágrafo 52 do Estudo Preliminar, visto que essa previsão não encontra respaldo na lei. Por esse motivo, a Abrafarma defende que o parágrafo 52 deve ser modificado, a fim de afastar a possível criação de uma obrigação adicional relacionada à reidentificação do titular e à reversão do processo de anonimização por terceiros.

- **Técnicas de anonimização e pseudonimização**. A ANPD identifica a substituição de dados, ofuscação de dados, criptografia, tokenização e mascaramento de dados como técnicas de pseudonimização (parágrafo 81 do Estudo Preliminar). Todavia, estas técnicas também podem ser aplicadas para fins de anonimização dos dados pessoais, à luz do Guide to Basic Anonymisation, da autoridade de proteção de dados de Singapura,[5] bem como do Anonymization Code of Practice, da autoridade de proteção de dados do Reino Unido.[6] A depender do "risco de reidentificação aceitável", o agente de tratamento seria capaz de empregar diversas técnicas para garantir a conformidade do processo com a LGPD e com as indicações da ANPD, de forma que essa informação poderia ser apresentada aos agentes diretamente no Guia Orientativo.

- **Etapas para a pseudonimização**. A ANPD parece impor diferentes etapas que devem ser observadas pelos agentes de tratamento, adotando linguagem que poderia indicar a atribuição de obrigações aos agentes de tratamento durante a condução do processo de pseudonimização (parágrafos 83 e 84 do Estudo Preliminar), sem qualquer correspondente na LGPD que imponha esses deveres aos agentes de tratamento. Recomenda-se que o posterior Guia Orientativo adote uma linguagem de recomendação de metodologias, para garantir maior segurança jurídica aos agentes de tratamento regulados – sem que haja a criação de obrigações adicionais para a adequação à LGPD nessa matéria. A Abrafarma entende que a adoção de uma linguagem recomendatória pela Autoridade garantiria maior segurança jurídica à condução dos processos de pseudonimização, sem que haja dúvidas quanto à criação de deveres adicionais para que os agentes estejam em conformidade com a LGPD.

---

[5] PDPC. "Guide to Basic Anonymisation". Disponível em:<https://www.pdpc.gov.sg/news-and-events/announcements/2022/03/guide-to-basic-anonymisation-now-available>. Acesso em: 26.02.2024.

[6] ICO. "Anonymization Code of Practice". Disponível em:<https://ico.org.uk/media/1061/anonymisation-code.pdf>. Acesso em: 26.02.2024.

- **<u>Meios automatizados no processo de anonimização</u>**. É possível que a anonimização ocorra apenas por meios automatizados, sem participação humana. Essa afirmação alinha-se diretamente ao artigo 5º, III, da LGPD, o qual prevê que um dado é anonimizado "considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento". Nesse sentido, a Abrafarma não concorda com a indicação da Autoridade de que a anonimização não deve ser totalmente automatizada (Apêndice I, "k", do Estudo Preliminar), à luz do próprio artigo 5º, III, da LGPD.

  A Abrafarma compreende que a LGPD permite que o agente de tratamento adote todos os meios viáveis à garantia do processo de anonimização, independentemente de eles terem a participação ou a intervenção de humanos, razão pela qual se defende a revisão da alínea "k" do Apêndice I do Estudo Preliminar.

- **<u>Fiscalização dos processos</u>**. A ANPD poderia indicar com maior precisão em seu Estudo Preliminar como ocorrerá a fiscalização dos processos de anonimização levados a cabo pelos agentes de tratamento regulados. Desse modo, poderia haver uma indicação específica por parte da Autoridade quanto à maneira mais indicada de documentação dos processos de anonimização, primordialmente com o intuito de garantir maior segurança jurídica nos projetos de adequação à LGPD dos agentes regulados.

- **<u>Uso compartilhado de dados anonimizados e pseudonimizados</u>**. O uso compartilhado de dados pseudonimizados, sem os seus identificadores, configura, para o destinatário dessas informações, coleta de dados anonimizados, conforme sustenta a autoridade de proteção de dados do Reino Unido.[7] Recomenda-se, com isso, que a ANPD inclua esse esclarecimento em seu Guia, especialmente para que o destinatário não seja responsabilizado pelos riscos relativos ao processo inicial de pseudonimização.

  No mesmo sentido, a Abrafarma compreende que o uso compartilhado de dados anonimizados não seria capaz de gerar a responsabilidade do destinatário pelos riscos relativos ao processo de anonimização previamente realizado a esse compartilhamento. Recomenda-se, portanto, que a ANPD preveja esse ponto especificamente em seu Guia de Anonimização e Pseudonimização, especialmente para garantir maior segurança jurídica ao destinatário das informações.

---

[7] ICO. "Introduction to Anonymisation". Disponível em:<https://ico.org.uk/media/about-the-ico/consultations/2619862/anonymisation-intro-and-first-chapter.pdf>. Acesso em: 26.02.2024.

São Paulo, 14 de março de 2024.

À
AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)
Coordenação-Geral de Normatização
A/C: Rodrigo Santana dos Santos
normatizacao@anpd.gov.br

Ref.: Consulta à sociedade sobre Estudo Preliminar – Anonimização e pseudonimização para proteção de dados

Prezados/as,

A **ASSOCIAÇÃO BRASILEIRA DE INTERNET – ABRANET** – pessoa jurídica constituída na forma de associação civil sem fins lucrativos, com sede na Rua MMDC, nº 450 cj. 304, São Paulo/SP, é uma entidade de classe sem fins lucrativos, fundada em 1996, para representar empresas pioneiras e inovadoras em serviços nativos da Internet, especialmente pequenos provedores de acesso à Internet, provedores de conteúdo, plataformas*, fintechs, paytechs* e data centers. De abrangência nacional, conta com mais de 400 (quatrocentas) associadas, tendo atuado como uma das principais fontes técnicas do setor junto ao Poder Público, sociedade civil e mercado, em apoio à proteção de dados, empreendedorismo, inovação, concorrência, simplicidade e democratização do acesso a produtos e serviços digitais.

Alguns exemplos ilustram a ampla atuação da ABRANET junto à ANPD, como: (i) apoio à aprovação e na construção da LGPD; (ii) apoio à criação da Autoridade Nacional de Proteção de Dados; (iii) envio de contribuições para a consulta pública sobre incidente de segurança com dados pessoais; (iv) envio de contribuições para a consulta pública sobre legítimo interesse; (v) envio de contribuições para a consulta pública sobre proposta de Regulamento sobre a atuação do Encarregado; e (vi) envio de contribuições para a consulta pública sobre sandbox regulatório de inteligência artificial e proteção de dados pessoais no Brasil.

Tendo em vista o exposto, a ABRANET possui profundo interesse em tecer comentários a respeito do Estudo Preliminar sobre Anonimização e Pseudonimização (“Estudo”), e congratula a Autoridade pela ampla abertura em dialogar com a sociedade e mercado em prol

do aprimoramento das políticas relacionadas à proteção de dados no Brasil. Passa-se, abaixo, às contribuições específicas da Associação.

As principais considerações levantadas pela ABRANET versam sobre:

(i) Instituto da anonimização não ser considerado uma operação de tratamento de dados pessoais;

(ii) Direito do titular de dados à anonimização restrito à hipótese do art. 18, IV da LGPD;

(iii) As etapas de pseudonimização;

(iv) Não haver vedação plena à anonimização totalmente automatizada;

(v) Criptografia típica como ferramenta suficiente de anonimização ou pseudonimização;

(vi) Agregação de dados como técnica de anonimização

(vii) Definição excessivamente ampla de “meios próprios” prevista no art. 12 da LGPD

(viii) Equiparação indevida de dados financeiros com dados pessoais sensíveis e criação de canal de consulta sobre anonimização; e

(ix) Adoção de medidas de segurança e transparência como atenuante em caso de reidentificação

Passa-se a essas considerações a seguir.

I. Anonimização não ser considerada operação de tratamento de dados pessoais

Em seu Estudo, a ANPD considera que o processo de anonimização configura uma operação de tratamento de dado pessoal comum, de modo a atrair os princípios e regras da LGPD, em especial os princípios da necessidade, finalidade e adequação. Este entendimento, no entanto, leva ao engessamento do instituto da anonimização. É dizer, ao considerar indistintamente a anonimização como operação de tratamento de dados pessoais, a ANPD acaba por dificultar, e até mesmo obstar, a utilização de um procedimento que é em sua natureza protetivo, sem grandes contrapartidas, resultando em um **incentivo negativo para os agentes de tratamento de dados pessoais adotarem essa medida.**

O Estudo traz a necessidade de informar preliminarmente ao titular da coleta dos dados que uma das finalidades do tratamento será a anonimização de seus dados, ou ainda, quando a finalidade não for informada ao titular no momento da coleta, a anonimização deve ser entendida como "tratamento subsequente" ou "uso secundário", e se limitar às finalidades explicitamente informadas ao titular de dados. A ABRANET considera esse entendimento e seus potenciais desdobramentos irrazoáveis e complicadores da prática, porque entende que **(i) a anonimização não é uma finalidade em si que necessita ser destacada, mas um meio para atingir determinada finalidade**, (ii) não há sentido em se exigir que se explicite a "finalidade" do tratamento de dados anonimizados, **uma vez que esses dados não são considerados pessoais** e; (iii) considerar o uso de dados anonimizados como "tratamento subsequente" ou "uso secundário" é admitir que, mesmo após a perda completa do vínculo com o titular de dados, ou seja, mesmo quando o dado é anônimo, a LGPD continuaria se aplicando, estendendo o escopo da norma contra o próprio texto da lei.

Ou seja, caso a anonimização fique sujeita a integridade do disposto na LGPD, ter-se-ia uma contradição em relação à própria Lei, uma vez que o seu art. 12 prevê que dados anonimizados não são considerados como dados pessoais para os fins da LGPD. Entender que que o procedimento de anonimização em si sujeita-se a todos os princípios da legislação de proteção de dados pessoais, não só no momento do processo de anonimização como também depois deste ter ocorrido, por sua vez, acarretaria a extensão indevida de seus efeitos aos dados resultantes da anonimização.

Nesse sentido, o Considerando/Recital 26 da *General Data Protection Regulation (GDPR)* prevê que *"**os princípios da proteção de dados não deverão aplicar-se** às informações anônimas, ou seja, às informações que não digam respeito a uma pessoa singular identificada ou identificável nem **a dados pessoais tornados de tal modo anónimos que o seu titular não seja ou já não possa ser identificado**"*.[1]

A interpretação sistemática da LGPD aponta que a anonimização constitui um processo técnico acessório às operações de tratamento de dados pessoais, e não uma operação de tratamento em si mesma: nos termos da Lei (art. 13), a anonimização e a pseudonimização são "práticas de segurança".

Assim, em verdade, ao equiparar a anonimização com o tratamento de dados, o Estudo caminha no sentido oposto ao do estímulo de práticas de salvaguarda dos dados pessoais, pois dificulta a realização do procedimento de anonimização. **A ABRANET sustenta, assim, que a anonimização não depende de base legal e a aplicação da principiologia da LGPD deve se referir à operação de tratamento de dados principal, e não, de forma específica e destacada, sobre o procedimento de anonimização e/ou pseudonimização**. Por fim, **a ABRANET reitera os riscos de se estender a aplicação do regime de proteção de dados para os dados anonimizados, o que resultaria em uma contradição normativa e em um comprometimento relevante do instituto da anonimização.**

II. Direito do titular de dados à anonimização restrito à hipótese do art. 18, IV da LGPD

O parágrafo 22 do Estudo prevê que há recomendação para uso da anonimização e da pseudonimização "*como um direito que o titular de dados possui, respectivamente, podendo requerer do controlador a anonimização de seus dados pessoais, quando esta é viável".* Convém explicitar, no entanto, que, em acordo com o disposto no art. 18, IV da LGPD a anonimização é um direito do titular apenas quando os dados são *"desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei".* A revisão do trecho é necessária para evitar interpretações divergentes ou extensivas. Em suma, **a ABRANET sugere a alteração para esclarecer que a anonimização é direito do titular em circunstâncias específicas.**

[1] 1 Disponível em: https://gdpr-text.com/pt/read/recital-26/. Acesso em: 22/02/2024.

III. Considerações sobre as etapas da pseudonimização

Considerando as informações apresentadas pelo Estudo no que diz respeito à metodologia para a eficaz pseudonimização, a ABRANET sugere que sejam consideradas algumas ressalvas sobre as etapas apresentadas.

Por exemplo, no ponto 10 "Avaliação de Impacto À Proteção de Dados", o Estudo versa sobre a elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD). É verdade que o Estudo indica a elaboração do RIPD apenas "quando apropriado", visando avaliar os riscos associados à pseudonimização e assegurar a conformidade com a LGPD. No entanto, é questionável se a inclusão no Estudo do RIPD como etapa "regular" do processo é necessária, tendo em vista que todas as preocupações relacionadas à proteção de dados podem ser adequadamente endereçadas nas demais fases trazidas o Estudo. Isso porque o RIPD, conforme as demais iniciativas regulatórias da ANPD, como por exemplo, o "Guia de Legítimo Interesse", é apontado como um importante instrumento de avaliação de riscos em casos em que esse risco possua uma probabilidade razoável de ser alto, o que não se vislumbra de plano em procedimentos de pseudonimização.

Nesse mesmo sentido, a ABRANET convida à reflexão sobre outras etapas que poderiam ser reconsideradas, que são: (i) Monitoramento e Auditoria; (ii) Treinamento e Conscientização; (iii) Registro e Documentação; (iv) Comunicação com os Titulares; (v) Plano de resposta a Incidentes de Segurança. Essas etapas fazem parte do contexto amplo e geral do tratamento de dados pessoais, sendo necessário reavaliar exigência específica ao processo de pseudonimização.

Assim, a ABRANET sugere a reavaliação da redação do Estudo, para reiterar que a **metodologia indicada no processo de pseudonimização não é vinculante**, especialmente considerando a proporcionalidade e eficácia da etapa no caso concreto da metodologia. Seria especialmente interessante esclarecer que a **elaboração do RIPD não é uma medida indispensável e proporcional para mitigar os riscos à privacidade dos indivíduos.**

IV. Não haver vedação plena à anonimização totalmente automatizada

O apêndice I do Estudo traz os "principais esclarecimentos" da ANPD sobre os procedimentos de anonimização e pseudonimização. O ponto (k) estipula expressamente que *"a anonimização não deve ser totalmente automatizada*". A redação segue prevendo, no entanto, que a intervenção de um especialista humano "poderá ser necessária", tendo em vista a importância do contexto e a avaliação geral do processo. Dessa forma, o texto abre margem para dúvidas sobre a necessidade da intervenção humana em todos os procedimentos.

A ABRANET considera que **não há razão para a intervenção humana na integralidade dos procedimentos de anonimização ou pseudonimização**, mesmo porque (i) em situações em que a base de dados é muito volumosa a intervenção humana nos processos pode inviabilizá-los ou, ainda, não ser necessariamente útil, vez que, dada a natureza da tarefa, essa somente poderá ser feita por amostragem e (ii) a LGPD não veda qualquer meio para anonimizar os dados, mas pelo contrário, autoriza todos os "meios técnicos razoáveis e disponíveis na ocasião de seu tratamento" (art. 5º, III).

Além do mais, a responsabilidade e os riscos sobre a correta realização dos procedimentos sempre serão do agente de tratamento, cabendo assim a eles determinarem os melhores métodos para a sua realização. Reconhece-se a possibilidade de haver, na prática, casos que, por sua natureza, necessitarão de algum grau de intervenção humana, como pedidos de titulares e investigações da ANPD, mas estes não representam a inteireza das vezes em que os procedimentos de anonimização e pseudonimização serão realizados e, mesmo que referida previsão seja omitida, na prática os agentes de tratamento de dados pessoais ainda estarão sujeitos a questionamentos e responsabilizações por seus procedimentos, mesmo que automatizados.

V. Criptografia típica como ferramenta suficiente de anonimização ou pseudonimização

Na seção de principais esclarecimentos, o Estudo restringe o uso da criptografia típica como técnica de anonimização, citando que esta não se enquadra propriamente nesse conceito, mas sim na modalidade de pseudonimização em razão da possível reversibilidade.

É relevante destacar que a criptografia pode atender aos requisitos de anonimização em determinados contextos, quando são utilizados algoritmos criptográficos unidirecionais.

Conforme mencionado pelo próprio Estudo, esses algoritmos podem atender os requisitos para serem considerados recursos de anonimização, pois tornam extremamente difícil ou inviável a reversão do processo, ao mesmo tempo em que garantem que os dados cifrados sejam úteis. Ademais, **a ABRANET compreende que a criptografia típica poderia ser considerada uma técnica de anonimização em razão de sua robustez e protetividade, consideravelmente mais altas quando comparadas a outras técnicas consideradas "adequadas" no Estudo sob o conceito de anonimização, possuindo um grau de reversibilidade significativamente menor.**

De tal forma, a ABRANET sugere que seja alterado o entendimento exposto nos esclarecimentos, **para que o Estudo abarque a criptografia típica como forma viável de anonimização,** não sendo necessário fazer a ressalva apresentada, considerando o nível de proteção e segurança oferecidos por essa técnica e dado que já é reconhecida a parcialidade de qualquer técnica de anonimização.

VI. Agregação de dados como técnica de anonimização

O Estudo não aborda de maneira detalhada a temática da agregação de dados, processo de coletar e agrupar dados em um formato compacto, resumindo, assim, grandes conjuntos de dados. Não fica claro se a ANPD considera este procedimento como uma técnica de anonimização – a técnica não é trazida expressamente no Apêndice II. Esclarecer este ponto é importante, pois dados agregados são muito utilizados em pesquisas, justamente uma das situações em que a própria LGPD recomenda o uso da anonimização (art. 7º, IV).

Considerando a natureza e a forma de constituição da **agregação de dados, a ABRANET a entende como uma forma de anonimização valiosa, que possui em muitos cenários baixo risco de reidentificação e que permite com que os agentes de tratamento possam utilizar dados para determinadas finalidades da forma menos intrusiva possível – resguardando não só a segurança como também a proteção destes dados pessoais.** Deste modo, **a ABRANET propõe que a agregação de dados seja explicitamente considerada técnica de anonimização, em prol da proteção de dados pessoais e segurança jurídica.**

VII. Definição excessivamente ampla de "meios próprios" prevista no art. 12 da LGPD

A compreensão dos termos "esforços razoáveis" e "meios próprios" previstos no artigo 12 da LGPD é fundamental para avaliar adequadamente os riscos de reidentificação e a reversão do processo de anonimização. Nesse sentido, é importante que as definições trazidas no Estudo sejam suficientemente claras e concretas. Parte dessa conceituação é construída pelos elementos exemplificados para garantir a anonimização. Outros elementos que poderiam ser caracterizados são as normas de conformidade e de governança de dados nas políticas internas das empresas.

Na visão da ABRANET, é necessário esclarecer a definição de "meios próprios", que parece ter sido interpretada de forma ampla no Estudo, abrangendo até mesmo meios de grupos de indivíduos e entidades. **Essa expansão do conceito pode enfraquecer a categorização do que seriam meios próprios**, perdendo sua distinção e razão de ser como qualificante, tal como previsto na LGPD. Uma definição mais precisa e delimitada é essencial para evitar interpretações equivocadas e para observância plena da intenção legislativa por detrás do dispositivo da LGPD. Assim, a ABRANET sugere que haja uma definição mais específica e restrita de meios próprios, alinhada com o disposto no art. 12 da LGPD.

VIII. Equiparação indevida de dados financeiros com dados pessoais sensíveis e criação de canal de consulta sobre anonimização

O Estudo propõe estabelecer uma abordagem baseada em risco, com base em cálculos do Risco de Reidentificação Mensurado (RRM) e do Risco de Reidentificação Aceitável (RRA). Enquanto é elogiável a robustez do Estudo, que é acompanhado de exemplos e casos concretos, é fundamental considerar as implicações práticas envolvidas nesse processo, visto que é gerada nova camada de complexidade ao procedimento de anonimização, criando cálculos discricionários dos agentes de tratamento envolvidos.

A proposta de quantificação do risco aceitável e do risco mensurado pode gerar responsabilizações desproporcionais para os agentes de tratamento, por exemplo, **quando considerada a equiparação de dados financeiros com dados pessoais sensíveis como fator agravante para diminuir o Risco de Reidentificação Aceitável**. Essa prática pode contrariar o regime estabelecido pela LGPD, uma vez que o legislador **optou por não incluir os dados**

financeiros dentro da categoria de dados sensíveis, tampouco resguardou-os a uma tutela especial e diferenciada em relação a dados pessoais "comuns". Ademais, é válido ressaltar que dentro da categoria "dados financeiros" há a possibilidade de enquadramento de informações que representam baixo risco e impacto aos titulares e que sejam pouco relevantes em concreto.

Outra fragilidade possível pela adoção desse tipo de cálculo discricionário é a divergência de compreensão entre agentes de tratamento e a ANPD, considerando que as diversas variáveis apresentadas no Estudo para a realização dos cálculos dificultam o consenso sobre o cálculo do risco em eventual processo de fiscalização ou sancionatório.

Ainda, a ABRANET sugere que a ANPD disponibilize um canal de consultas facilitada para orientar os agentes na estruturação de seus programas de anonimização, especialmente voltado para agentes de pequeno porte que não possuem capacidade técnica, informacional ou financeira para se adequar aos padrões estabelecidos pela ANPD. Essa medida seria essencial para promover a conformidade com a LGPD e reduzir as incertezas e dificuldades enfrentadas pelos agentes de tratamento. Essa abordagem permitiria uma análise mais abrangente e contextualizada dos riscos envolvidos na anonimização, sem a necessidade de cálculos discricionários aos agentes de tratamento.

Caso a ANPD entenda conveniente a realização de uma "filtragem" das solicitações de consulta, é possível considerar um sistema que permitiria que entidades e associações setoriais possam encaminhar questões à ANPD, após demonstrarem o interesse geral de sua consulta (em detrimento de possível interesse particular do agente de tratamento individual), de modo a obter uma resposta satisfatória e geral para os seus representados. **Por fim, a ABRANET é contrária à equiparação de dados financeiros com dados pessoais sensíveis, para quaisquer finalidades, por afronta ao art. 5, II da LGPD.**

IX. Adoção de medidas de segurança e transparência como atenuante em caso de reidentificação

O Estudo diversas vezes evidencia que a anonimização de dados não assegura uma irreversibilidade total, o que reforça a necessidade de cautela e rigor na implementação de

políticas de proteção de dados e as diversas consequências decorrentes da reidentificação de dados.

Nesse sentido, a implementação de medidas que possam prevenir e mitigar os riscos associados à reidentificação de dados é um dos resultados dos investimentos no desenvolvimento de diretrizes e na promoção de melhores práticas.

A ABRANET sugere que a ANPD considere a adoção de medidas de segurança e transparência pelos agentes de tratamento como atenuantes em casos de reidentificação de dados, como forma de incentivar a adoção de boas práticas.

***

Sendo o que cumpria para o momento, a ABRANET coloca-se à disposição da ANPD para qualquer colaboração que esta venha a julgar necessária e apresenta seus protestos de elevada estima e consideração.

Atenciosamente,

ASSOCIAÇÃO BRASILEIRA DE INTERNET – ABRANET

O **INSTITUTO BRASILEIRO DE ESTUDOS DE CONCORRÊNCIA, CONSUMO E COMÉRCIO INTERNACIONAL – IBRAC**, associação civil sem fins lucrativos, inscrita no CNPJ sob o nº 96.287.453/0001-10, com sede em Rua Cardoso de Almeida, 788, cj. 121 – Perdizes, CEP 05013-00, São Paulo/SP, vem por meio deste apresentar as suas considerações em resposta à consulta à sociedade sobre o **Estudo Técnico de Anonimização e Pseudonimização** da ANPD.

O Ibrac é uma entidade privada, sem fins lucrativos, criada em dezembro de 1992, com o objetivo de promover a realização de pesquisas, estudos e debates sobre temas relacionados à defesa da concorrência, comércio internacional, consumo e regulação.

O interesse em contribuir para a consulta da ANPD surgiu do empenho comum dos membros do Comitê de Mercados Digitais e Dados em buscar a construção de um melhor ambiente jurídico de proteção de dados pessoais para os agentes econômicos envolvidos e o desenvolvimento de uma cultura de proteção de dados sólida, estável e robusta. Espera-se, assim, que as contribuições possam colaborar para a Consulta à Sociedade.

Sendo o que havia para o momento, nos colocamos à inteira disposição desta coordenação para quaisquer esclarecimentos adicionais

Contribuição do IBRAC sobre o Estudo Técnico de Anonimização e Pseudonimização da ANPD

De início, o IBRAC saúda a receptividade e disponibilidade da Coordenação Geral de Normatização da ANPD em considerar as contribuições da sociedade civil e do setor privado a respeito de um tópico de tamanha relevância prática e teórica para o âmbito da proteção de dados pessoais e para a estruturação e consolidação do regime jurídico da Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil. Deste modo, o IBRAC também reconhece os esforços da autoridade traduzidos na elaboração deste guia.

A fim de contribuir para este esforço, o instituto apresenta alguns comentários. Os dois principias pontos de nossa contribuição recaem sobre aspectos teóricos - com intensas repercussões práticas - trabalhados no texto, qual sejam: (i) a anonimização como operação de tratamento de dados pessoais “comum” e; (ii) a distinção entre teoria objetiva x teoria subjetiva no que tange aos riscos de reidentificação e o enquadramento da LGPD. Ademais, ainda no cerne de nossa contribuição, aponta-se uma análise das técnicas apresentadas nos documentos juntados à consulta. Por fim, merecem comentários alguns outros pontos, que serão abordados abaixo de maneira mais específica.

1. Anonimização de dados e categorização como operação de tratamento de dados pessoais

O documento retrata o entendimento de que o processo de anonimização é um processo de tratamento de dados pessoais, e que por esse motivo estaria sujeito aos princípios e regras da LGPD. Aborda expressamente, nesse sentido:

(i) a necessidade de atendimento ao princípio da finalidade e da transparência com relação ao procedimento de anonimização, indicando que, se a finalidade da anonimização não guardar relação com as finalidades anteriormente informadas aos titulares, a anonimização em si seria um "tratamento posterior" ou uso secundário (itens 34 e 35);

(ii) a necessidade de atendimento ao princípio da adequação, exigindo que o procedimento de anonimização seja compatível com finalidades legítimas, específicas e explicitamente informadas ao titular;

(iii) a necessidade de se observar, ainda, o princípio da necessidade, limitando o tratamento (anonimização) ao mínimo necessário para se alcançar as finalidades especificadas.

Embora certamente não nos pareça incorreto considerar que a anonimização em si seja um processo de tratamento de dados, entendemos que essa abordagem poderá gerar um efeito contraditório com a própria lógica da LGPD, a depender de sua interpretação. Em termos práticos, se a anonimização ficar sujeita aos exatos mesmos princípios, o efeito seria estender a aplicação da LGPD aos dados anonimizados, contrariando disposição expressa do art. 12 da lei.

O procedimento de anonimização (quando realizado de forma apropriada e em conformidade com os requisitos da LGPD) está mais próximo da exclusão que das demais atividades de tratamento. O dado anonimizado, a partir de concluído o processo de anonimização, não se sujeita à LGPD, exatamente por não ser dado pessoal. Assim, o entendimento de que o procedimento de anonimização em si sujeita-se a todos os princípios da LGPD não deve implicar em estender os efeitos da lei aos dados resultantes da anonimização.

Caso contrário, não haveria incentivos suficientes para os agentes de tratamento de dados pessoais prosseguirem com a adoção e estruturação dos onerosos procedimentos de anonimização de dados pessoais – que no limite tem o condão de proteger os titulares de dados. Além disso, cumpre também destacar que isso implicaria sobrepor e fragilizar dispositivo legal expresso por meio de ato infralegal.

Desta maneira, o IBRAC entende que essa previsão precisa ser interpretada de maneira adequada, a fim de não ser **contrária** à boa construção de uma cultura de proteção de dados no Brasil, vez que desincentivaria a adoção da importante medida de segurança da anonimização de dados pessoais.

2. Teoria objetiva vs. Teoria subjetiva no risco de reidentificação dos dados.

O Estudo Técnico (pp. 14 e seguintes) pondera que o Brasil não teria aderido completamente à teoria objetiva (que considera como critério para medir o risco de reversão da anonimização os meios detidos por terceiros). Entretanto, o Estudo Preliminar caminha fortemente no sentido de que o critério para a apuração dos riscos de reversão da anonimização deve considerar os meios detidos por terceiros.

Consideramos que, neste aspecto, os estudos devam considerar mais explicitamente que a LGPD optou pela não adesão irrestrita à teoria objetiva, e que a interpretação dos efeitos do art. 12 (e de seu §1º) devam sim considerar critérios mais restritos de razoabilidade no acesso aos meios para reversão. O risco está principalmente numa interpretação de que o escopo das análises sempre devam considerar o nível mais alto de risco e de capacidade disponíveis, a "elite do estado da arte" (big techs, órgãos de inteligência etc.), limitando excessivamente o que deve ser considerado dado anonimizado e, consequentemente, expandindo exponencial e desproporcionalmente o que deve ser considerado para as possibilidades de reversão nos casos concretos.

Dado que a própria ANPD reconhece que a LGPD não aderiu totalmente à teoria objetiva, entendemos que alguns parâmetros adicionais de avaliação deveriam ser considerados para análise do caso concreto. Por exemplo, se o compartilhamento (lícito) é feito com agente que possua maior ou menor capacidade de reversão, o risco deve considerar as capacidades dos recipientes desses dados. Deste modo, sugere-se que a ANPD reflita sobre meios de se tornar mais equânime e proporcional a consideração acerca do risco de reversão para diferentes agentes, levando em conta seus riscos, seu porte, suas atividades e a sua exposição.

3. Estudo de casos sobre anonimização de dados na LGPD e a experiência internacional

Em relação ao estudo prático sobre os casos de uso, o Instituto entende que seria recomendável um aprofundamento nas questões práticas e implicações – inclusive em falhas e riscos – de cada técnica de anonimização. Para fins meramente exemplificativos, é possível considerar o "Opinion 05/2014 on Anonymisation Techniques" do Article 29 Data Protection Working Party como um parâmetro.

Rrecomenda-se a criação de um Apêndice ou Tópico no "APÊNDICE II - CADERNO DE TÉCNICAS PARA ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO" (pg.30) incluindo informações técnicas sobre boas práticas, erros comuns e riscos associados a cada tipo de técnica de anonimização e pseudonimização.

Tendo em vista que a ANPD reconhece como necessária a análise casuística e contextual de cada situação concreta e de cada conjunto de dados, sendo ônus dos agentes de tratamento de dados pessoais aferirem as situações concretas em mais detalhe, a adição seria de fundamental importância para reforçar a função educativa e orientativa do material, facilitando a construção e aplicação das melhores práticas de anonimização e, por conseguinte, norteando os agentes para a escolha das melhores estratégias para sua organização.

4. Outros apontamentos

a) **Desnecessidade da elaboração de RIPD no procedimento de pseudonimização:** O Ibrac aponta ressalvas em relação às etapas apresentadas para a eficaz pseudonimização, conforme detalhado no Estudo. Em especial, no ponto 10, que trata da Avaliação de Impacto à Proteção de Dados, o Estudo menciona a elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD). Embora o Estudo sugira a elaboração do RIPD apenas "quando apropriado", para avaliar os riscos associados à pseudonimização e garantir a conformidade com a LGPD, na prática essa disposição, sem maiores qualificações, leva os agentes de tratamento a entender que, por premissa, o RIPD deverá ser feito, uma sugestão que, em concreto, não encontra razão de ser. Há inúmeros casos em que a pseudonimização será um procedimento sem maiores riscos, e que elaborar um relatório seria inclusive contraproducente. Considerando o contexto de outras regulamentações e normatizações da ANPD, há um desalinho em relação à sugestão do RIPD em tratamentos de baixo impacto, uma vez que tal instrumento - de onerosa elaboração pelos agentes - vêm sendo recomendado para casos de tratamento que impliquem alto risco.

b) **Vedação à anonimização automatizada:** Expressamente, o ponto (k) do Apêndice I estipula que "a anonimização não deve ser totalmente automatizada", sugerindo que a intervenção de um especialista humano "poderá ser necessária" devido à importância do contexto e à avaliação geral do processo. Isso levanta questionamentos sobre a indispensabilidade da intervenção humana em todos os procedimentos. O Ibrac entende que não há justificativa para exigir a intervenção humana em todos os procedimentos de anonimização ou pseudonimização. Em casos de bases de dados volumosas, a intervenção humana pode inviabilizar os processos, e, além disso, a LGPD não proíbe qualquer método de anonimização, mas sim autoriza todos os "meios técnicos razoáveis e disponíveis na ocasião de seu tratamento" (art. 5º, III). Por fim, é importante salientar que a responsabilidade e os riscos associados à correta realização dos procedimentos é um pressuposto da responsabilidade do agente de tratamento, incumbindo-lhes determinar os melhores métodos para sua execução.

c) **Criptografia típica como uma forma de anonimização:** Na seção de principais esclarecimentos, o Estudo classifica a criptografia típica como uma forma de pseudonimização devido à sua reversibilidade potencial. No entanto, em determinados contextos, algoritmos criptográficos podem atender aos critérios de anonimização muito melhor do que as técnicas apresentadas como “boas práticas de anonimização” no Estudo, tornando extremamente difícil ou inviável reverter o processo. Nesse sentido, propõe-se uma revisão no entendimento apresentado no Estudo para incluir a criptografia típica como uma opção viável de anonimização,

eliminando a ressalva inicialmente feita, uma vez que já se reconhece a limitação inerente a qualquer técnica de anonimização ao longo do documento.

d) **Falta de orientações específicas sobre dados agregados e sobre a gestão da anonimização no tempo:** O Estudo não aborda a temática da agregação de dados, que envolve o processo de coleta e agrupamento de dados para resumir conjuntos volumosos. Não há clareza se a ANPD considera esse processo como uma técnica de anonimização ou pseudonimização, pois não é mencionado explicitamente no Apêndice II. Esclarecer essa questão é fundamental, especialmente porque os dados agregados são comumente empregados em pesquisas, uma das situações recomendadas pela LGPD para a aplicação da anonimização (art. 7º, IV). Além disso, considerando a anonimização como um processo contínuo e iterativo, faz-se necessária uma melhor orientação aos agentes de tratamento sobre a forma como esse processo deve ser conduzido ao longo do tempo, como por exemplo, periodicidade e método de reavaliações.

I. INTRODUÇÃO

Respeitando a agenda regulatória do biênio 2023-2024, publicada em 04 de novembro de 2022 (Portaria ANPD n. 35), a Autoridade Nacional de Proteção de Dados disponibilizou recentemente Estudo Preliminar sobre Anonimização e Pseudonimização para a proteção de dados pessoais, estudo este que submete a contribuições da sociedade no tema. Este estudo é o resultado da junção do Estudo Técnico sobre a anonimização de dados na LGPD: análise jurídica, o Estudo Técnico sobre a anonimização de dados na LGPD: Uma visão de processo baseado em riscos e técnicas computacionais e o Estudo de casos sobre anonimização de dados na LGPD.

Trazemos abaixo, portanto, os principais pontos de atenção que, em nossa opinião, ainda merecem maiores esclarecimentos pela Autoridade, objetivando subsidiar a compreensão da associação sobre o assunto.

De forma resumida, os principais pontos de atenção da norma, em nossa visão, são:

II. QUANTO A DEFINIÇÃO DE IDENTIFICADOR INDIRETO (2.1.)

SUGESTÃO DE ADIÇÃO
Roga-se à Autoridade que deixe explícito que, ao definir "Identificador indireto" ao se referir a dados anonimizados no Glossário de seu Estudo Preliminar, altere o termo "dados auxiliares" para "dados complementares", evitando, desse modo, confusão de terminologia com as bases de dados segregadas no processo de pseudonimização.

III. QUANTO A INCIDÊNCIA DE PRINCÍPIOS E DEVERES DA LGPD (2.2.)

SUGESTÃO DE ADIÇÃO
Roga-se à Autoridade que deixe explícito que a incidência de princípios e deveres da LGPD no processo de anonimização, tais como manutenção dos registro das operações de tratamento de dados pessoais e aplicação de base legal para uso legítimo de dados pessoais, somente deve ocorrer em dados que ainda não passaram pelo processo de anonimização. Isso porque dados anonimizados já não se enquadram mais no escopo da norma, em conformidade o art. 12 da norma.

IV. QUANTO A APLICABILIDADE DOS PRINCÍPIOS E DEVERES DA LGPD AO PROCESSO DE ANONIMIZAÇÃO (item 3.1.1.)

SUGESTÃO DE ADIÇÃO
Roga-se à autoridade que deixe explícito que a observância dos princípios da LGPD, bem como, da realização da avaliação descrita no parágrafo 37 do estudo, são ações a serem realizadas previamente a aplicação das técnicas de anonimização. Uma vez estas sendo bem-sucedidas, não haveria necessidade de compatibilizar as finalidades originárias de tratamento dos dados pessoais com os usos que os agentes de tratamento pretendem realizar com a base de dados anonimizada, uma vez que os dados anonimizados não estão sob o âmbito da incidência da LGPD.

V. QUANTO AO RISCO DE REINDENTIFICAÇÃO (item 3.1.2.)

SUGESTÃO DE ADIÇÃO
Roga-se à autoridade que apresente o risco de reindendificação por meio da análise de casos que exponham técnicas mais aderentes a realidade do mercado, com exemplos que tratem de banco de dados não estruturados, e que se utilizam de técnicas sofisticadas de anonimização, como aquelas baseadas no uso de inteligência artificial.

VI. QUANTO AS NOÇÕES DE ESFORÇOS RAZOÁVEIS E MEIOS PRÓPRIOS (item 3.1.3)

PEDIDO DE ESCLARECIMENTO
Roga-se à autoridade o esclarecimento quanto aos aspectos que ela valorativamente poderá considerar para densificar o conceito de esforços razoáveis. Adicionalmente, requer-se o esclarecimento sobre a necessidade de análise de esforços de terceiros, quando o art.12 caput e §1º LGPD vincula a análise de reindentificação exclusivamente ao uso de meios próprios.

VII. QUANTO A CRIAÇÃO DE SANDBOX REGULATÓRIO (3.2.)

SUGESTÃO DE ADIÇÃO
Recomenda-se a criação de sandbox para testagem da eficácia da anonimização com agentes de demais setores. Este cenário mostra-se interessante para os casos de anonimização de dados na saúde. As técnicas de reidentificação poderiam ser aplicadas sobre uma base de dados do SUS, por exemplo.

VIII. QUANTO A QUALIDADE DO DADO ANONIMIZADO (3.2.1.)

SUGESTÃO DE ADIÇÃO
Recomenda-se que a Autoridade também se refira à qualidade do dado anonimizado. Mesmo nos casos em que a anonimização seja a fase final do ciclo de vida do dado, é importante considerar um fator de diminuição da qualidade do dado em razão do tempo decorrido entre a anonimização e o momento de uso do dado. Este nível de qualidade do dado deve ser considerado nos casos de pesquisas, tratamento de dados de menores e grupos vulneráveis, e no treinamento de modelos algorítmicos, para evitar vieses causados por (i) banco de dados ou (ii) por repetição de banco de dados anonimizados com pouca variação.

IX. QUANTO A CRIAÇÃO DE DIRETRIZES DE MELHORES PRÁTICAS COM ÓRGÃOS REGULADORES (3.2.1.)

SUGESTÃO DE ADIÇÃO
Recomenda-se que a ANPD crie diretrizes de melhores práticas de anonimização e pseudonimização com contribuição da sociedade, como aquelas que forem firmadas setorialmente por órgãos reguladores que contem com ampla participação de agentes de tratamento.

X. QUANTO A GESTÃO DO RISCO DE REINDENTIFICAÇÃO (3.2.2.)

SUGESTÃO DE ADIÇÃO AO PARÁGRAFO 63
Este processo é apenas uma das diferentes possibilidades existentes que o agente de tratamento poderá se amparar para avaliar o risco de reindentificação de determinado processo de anonimização, inclusive, mas não se limitando a análises não probabilísticas, como as análises contextuais.

SUGESTÃO DE ADIÇÃO
Roga-se à autoridade que deixe explícito o caráter meramente orientativo e sugestivo da proposta de processo de anonimização baseada em riscos indicada no item 3.2.2, de modo a não afetar a liberdade dos agentes de tratamento em escolher a técnica, o modelo, o procedimento e o tipo documental adequado ao contexto do tratamento dos dados objeto da anonimização.

XI. QUANTO A SEPARAÇÃO DE BASES DE DADOS NO PROCESSO DE PSEUDONIMIZAÇÃO (3.3.)

SUGESTÃO DE ADIÇÃO
Um dos requisitos essenciais para a aplicação da técnica de pseudonimização é que as informações adicionais necessárias para reverter o processo sejam mantidas pelo controlador de forma segregada, em um ambiente controlado e seguro. Contudo, há uma lacuna em relação ao significado preciso de "manter separadamente". Roga-se à Autoridade que o texto forneça detalhes claros sobre os critérios de armazenamento dos dados auxiliares, delineando de forma objetiva como essa separação deve ser realizada, como, por exemplo, a obrigação de separar os dados auxiliares em um banco de dados ou sistema de armazenamento diferente dos dados pseudonimizados.

XII. DA DIFERENCIAÇÃO DE TÉCNICAS DE PSEUDONIMIZAÇÃO E ANONIMIZAÇÃO (3.3.)

SUGESTÃO DE ADIÇÃO
Roga-se à autoridade que se aprofunde na explicação pormenorizada de cada técnica de pseudonimização em contraposição com as técnicas de anonimização de dados. Aponta-se como exemplo a técnica de mascaramento, conforme item 81 "e", no qual é citado tanto em técnicas de pseudonimização, quanto anonimização. Entende-se que é importante que a ANPD indique em quais momentos a mesma técnica poderá distinguir-se de outra. Compreende-se pela pertinência, ainda, que a Autoridade realize a indicação de um rol exemplificativo das técnicas de anonimização e pseudonimização, inclusive, incluindo técnicas mais aderentes à realidade do mercado e com a utilização de ferramentas de tecnologia, conforme estado da arte atual.

XIII. DA GARANTIA AOS DIREITOS DOS TITULARES EM RELAÇÃO A DADOS PSEUDONIMIZADOS (3.3.)

SUGESTÃO DE ADIÇÃO
Roga-se à Autoridade que forneça diretrizes quanto às obrigações dos agentes de tratamento em relação às respostas às solicitações de titulares de dados eventualmente pseudonimizados. Como exemplo, compreende-se que, apesar dos apontamentos realizados em sede de Estudo Preliminar, permanece incerto se, eventualmente, no caso dos dados pseudonimizados, o controlador precisará reverter a pseudonimização para viabilizar o exercício dos direitos dos titulares.

XIV. DA NECESSIDADE DE INTERVENÇÃO HUMANA NO PROCESSO DE ANONIMIZAÇÃO (APÊNDICE I)

SUGESTÃO DE ADIÇÃO
Roga-se à Autoridade que esclareça quais aspectos deverão ser considerados pelos agentes de tratamento para estabelecer a necessidade de intervenção humana em procedimentos de anonimização, indicando quais os parâmetros devem ser considerados por estes para definição da importância de participação humana no processo.

CONSULTA À SOCIEDADE - ESTUDO PRELIMINAR - ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO PARA PROTEÇÃO DE DADOS

CONTRIBUIÇÕES

Com base no estudo preliminar disponibilizado pela ANPD a respeito da anonimização e pseudonimização de dados e, ainda, nos documentos adicionais disponibilizados, elaboramos as presentes sugestões e dúvidas, a respeito das quais tomamos a liberdade de elencarmos todas em tópicos individuais ligados ao documento a que fazem menção:

ANÁLISE ESTUDO PRELIMINAR ANPD:

1) O estudo não toma em consideração a existência de diversas estruturas de empresas: tanto pequenas quanto grandes. Desta forma, o contexto de "meios razoáveis" para anonimização/pseudonimização é muito amplo e aberto e pode gerar precedentes diversos/insegurança jurídica.

2) Ainda tomando em consideração o contexto geral do documento elaborado, quais métodos são homologados/chancelados, inclusive seguindo as melhores práticas internacionais, para anonimização e pseudonimização de dados?

3) No item 44 (página 14), os documentos falam em "ataques de reidentificação" com empréstimo do termo "ataque" da literatura especializada. Contudo, o termo "ataque" não é usado na legislação aplicável. Sugerimos o emprego do termo "incidente" nesse caso, uma vez que o uso de termo emprestado parece fugir ao rigor técnico necessário.

4) Quanto ao diagrama "utilidade x anonimização" disponibilizado na página 17, identificam-se situações nas quais se pode ter anonimização e utilidades máximas simultaneamente, sem que existam, necessariamente, concessões em cada uma dessas áreas. Por conta disso, entendemos que nem sempre a lógica esboçada pelo diagrama será verificável, uma vez que varia de acordo com cada caso prático.

5) A orientação sugere, ainda, em vista do estabelecido na página 20, critérios objetivos (equação matemática) para mensuração do risco de reidentificação pós-anonimização. No entanto, a própria anonimização aparenta ser um conteúdo subjetivo (varia de acordo com cada caso). Faz sentido, nesse contexto, manter uma equação matemática para solução de uma situação com estas características?

6) No diagrama da página 23 (Metodologia Eficaz de Pseudonimização), será que os itens 11 e 12 deveriam mesmo ser incluídos ao final dele numa ordem sequencial? Devem sempre fazer parte desta linha de raciocínio? Não seriam pontos adicionais que, embora preparados,

ficam apartados do restante? Ainda, o monitoramento e auditoria não deveriam ser incluídos apenas depois do integral treinamento e conscientização da empresa?

7) Por fim, em uma linha geral de reflexão: e se o tratamento que está sendo realizado diga respeito a presos ou pessoas em situação de vulnerabilidade equivalente? Seria necessário um grau de anonimização ou pseudonimização mais robusto? O documento não se manifesta a respeito.

ESTUDO TÉCNICO SOBRE ANONIMIZAÇÃO DE DADOS NA LGPD: UMA VISÃO DE PROCESSO BASEADO EM RISCO E TÉCNICAS COMPUTACIONAIS

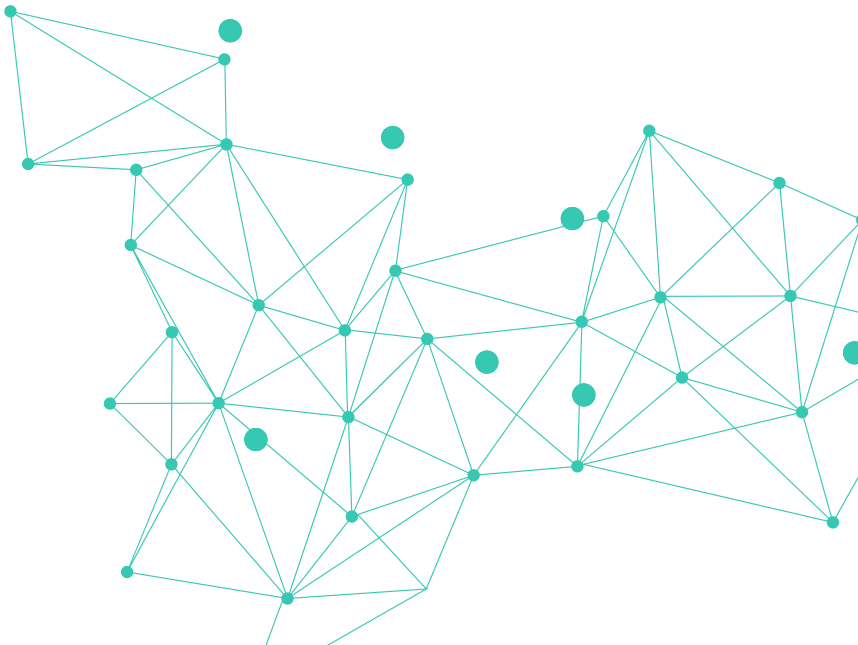
1) Tomando em consideração que o documento embasou os demais documentos produzidos, sentimos falta, no conteúdo principal, da informação a respeito da importância em se realizar a devida documentação das etapas de anonimização dos dados. Seria interessante a inclusão deste ponto de maneira mais clara no documento final (Estudo Preliminar ANPD);

ESTUDO TÉCNICO SOBRE A ANONIMIZAÇÃO DE DADOS NA LGPD: ANÁLISE JURÍDICA:

1) Acredito que nesse ponto o estudo confunde “metodologia” com “recursos metodológicos”. A metodologia, via de regra, se encaixa em determinadas categorias pré-estabelecidas (método argumentativo, lógico-argumentativo, hipotético-dedutivo, etc.). Além disso, considerando que o documento não clarifica quais conceitos deverão ser adotados pelos agentes de tratamento, é importante que seja definido qual o padrão que será adotado pelos agentes no Brasil.

Peck Advogados

Consulta à Sociedade - Estudo Preliminar - Anonimização e pseudonimização para proteção de dados



Rua Henrique Schaumann, 270 – 4° andar
São Paulo (SP) CEP 05413-909
Tel: 11 2189 0444
www.peckadv.com.br | contato@peckadv.com.br

Consulta à Sociedade

Estudo Preliminar - Anonimização e pseudonimização para proteção de dados

À AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS ("ANPD")

Prezados,

O Peck Advogados vem, por meio desta, apresentar as suas considerações técnicas e legais em resposta à abertura, realizada pela ANPD em 30/01/2024, da tomada de subsídios acerca do Estudo Preliminar - Anonimização e pseudonimização para proteção de dados.

A referida tomada de subsídios tem, como finalidade, receber contribuições de profissionais da área, dos agentes de tratamento, de titulares, do setor acadêmico e da sociedade em geral, de modo a permitir uma atuação regulatória alinhada às melhores práticas e à realidade.

1. Considerando o conteúdo do Estudo Preliminar, apresente suas contribuições sobre o texto.

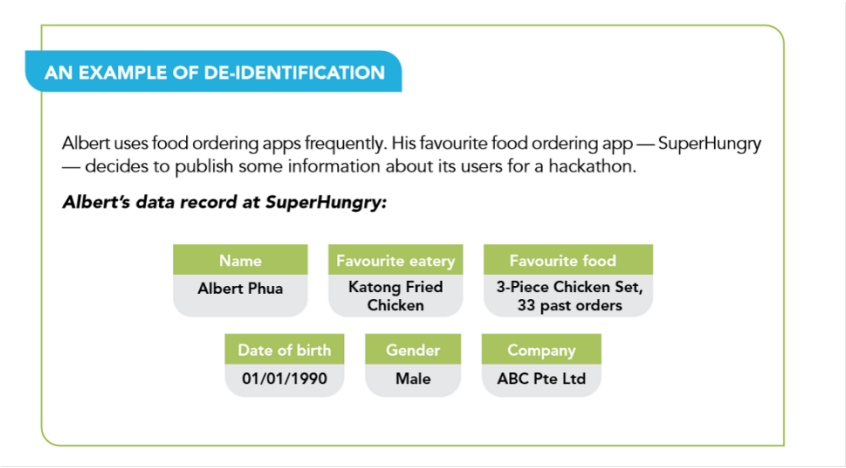
Contribuição (300 caracteres): Incluir quadro exemplificativo itens 13 -15. Conveniência da anonimização, não será exigida do controlador (item 22). Item 58 se efetivamente ocorrer a anonimização, não haverá aplicação da legislação. Item 71, L-Diversidade e a T-Proximidade. Item 3.2 citar Dados Sintéticos e Princípio da Exaustão.

Considerações:

Considerando que anonimização e pseudonimização são duas técnicas distintas que permitem o uso de dados não identificados, residindo diferença entre as duas técnicas na possibilidade de os dados serem reidentificados ou não. Em que pese, que tenha sido disposto no presente Estudo Preliminar disposições jurídicas pertinentes sobre

padrões de aplicação de técnicas para o processo de anonimização e pseudonimização, necessário maior clareza quanto aplicação das etapas destes processos, mormente, seguem sugestões de aprimoramento do Estudo disponibilizado visando maior abrangência prática pelos agentes de tratamento:

Os parágrafos 13 - 15 tratam sobre identificadores diretos e indiretos. Nesse aspecto, levando em consideração o Guia de Anonimização elaborado pela Comissão de Proteção de Dados Pessoais de Singapura, recomendamos a inclusão de quadro exemplificativo em movimento similar ao que vemos em outros guias da ANPD.



Pag. 7 do Guia Básico para Anonimização, PDPC, Singapura.

Quanto ao parágrafo 22 do estudo, a orientação da ANPD deva ser complementada a fim de expressamente reconhecer que, diante do elevado grau de dificuldade técnica que envolve o processo de anonimização e pseudonimização, a sua realização não poderá ser exigida incondicionalmente do controlador. Nos casos de "estudo por órgão de pesquisa" e "estudos em saúde pública", previstos pela LGPD, há expressa menção à conveniência da anonimização, de modo que se entende que o legislador estabeleceu que tal obrigação não será exigida do controlador.

O parágrafo 58 determina que compete ao agente de tratamento identificar o grau de utilidade do dado pessoal para alcançar a finalidade especificada, e em consequência estabelecer o grau necessário de anonimização dos dados. No entanto, o próprio estudo estabelece que não há aplicação da LGPD aos dados anonimizados, ou seja, independentemente da finalidade do tratamento, se efetivamente ocorrer a

Rua Henrique Schaumann, 270 – 4° andar
São Paulo (SP) CEP 05413-909
Tel: 11 2189 0444
www.peckadv.com.br | contato@peckadv.com.br

anonimização, não haverá a aplicação da legislação. Logo, o texto leva a ideia de que o controlador deveria aplicar técnicas de pseudonimização e não de anonimização.

O parágrafo 71 do estudo, remete a ideia de combinar o k-anonimato a L-Diversidade e a T-Proximidade. No entanto, o texto não aborda os conceitos de referidas técnicas ou exemplos da aplicação, no Apêndice III. Nesse sentido, recomendamos inserir os conceitos de L-diversidade, que se trata de uma extensão do k-anonimização que garante que haja variação (L=2, por exemplo) em um atributo sensível, enquanto a T-Proximidade garante que a distribuição de um atributo sensível dentro da generalização de um quase-identificador aproxima-se da distribuição do atributo sensível em todo o conjunto de dados (Disponível em: https://utrechtuniversity.github.io/dataprivacyhandbook/k-l-t-anonymity.html. Acesso em: 26/02/2024).

Do mesmo modo, o texto não faz menção a Privacidade Diferencial, que é uma tecnologia de aprimoramento de privacidade (PETs). Trata-se de uma abordagem que objetiva proteger a privacidade dos indivíduos ao compartilhar informações sobre um grupo de indivíduos, descrevendo os padrões encontrados na base de dados enquanto retém informações sobre indivíduos específicos por meio de alterações que não alteram a estatística de interesse. A privacidade diferencial é uma ferramenta importante quando se trata de IA e machine learning. (Disponível em: https://www.nist.gov/news-events/news/2023/12/nist-offers-draft-guidance-evaluating-privacy-protection-technique-ai-era. Acesso em: 26/02/2024). Disponível em: https://privacytools.seas.harvard.edu/differential-privacy. Acesso em: 26/02/2024)).

O Item 3.2 dispõe sobre a Anonimização, mas não faz diferenciação ao leitor sobre a utilização de anonimização estática, na qual o banco de dados se torna anônimo em sua totalidade, e anonimização dinâmica, quando aplicada dinamicamente à medida em que os dados são consultados, com técnicas de adição de ruídos e técnicas de mascaramento dos resultados.

Além disso, o guia orientativo não recomenda ou faz menção ao uso de dados sintéticos, que são aqueles dados gerados artificialmente que têm aproximadamente as mesmas

Rua Henrique Schaumann, 270 – 4° andar
São Paulo (SP) CEP 05413-909
Tel: 11 2189 0444
www.peckadv.com.br | contato@peckadv.com.br

propriedades dos dados brutos, mas isso não permite que conclusões sejam tiradas sobre os indivíduos no conjunto de dados original.

Por outro lado, considerando a inteligência artificial, o aprendizado de máquina deve observar o Princípio da Exaustão. Trata-se de uma exceção a utilização da anonimização, que objetiva fornecer informação máxima e completa, sem a utilização qualquer técnica de anonimização ou dados sintéticos, para que o algoritmo seja capaz de aprender na sua completude, mitigando os riscos de viés e alucinação. Nestes casos, a anonimização seria aplicada posteriormente, no uso para a finalidade pretendida. Alguns exemplos da aplicação do Princípio da Exaustão são, p. ex., o treinamento de inteligência artificial para as áreas da saúde, poder judiciário e segurança pública.

2. Gostaria de deixar algum comentário ou sugestão adicional?

(para inserir anexos - usar e-mail : normatizacao@anpd.gov.br)

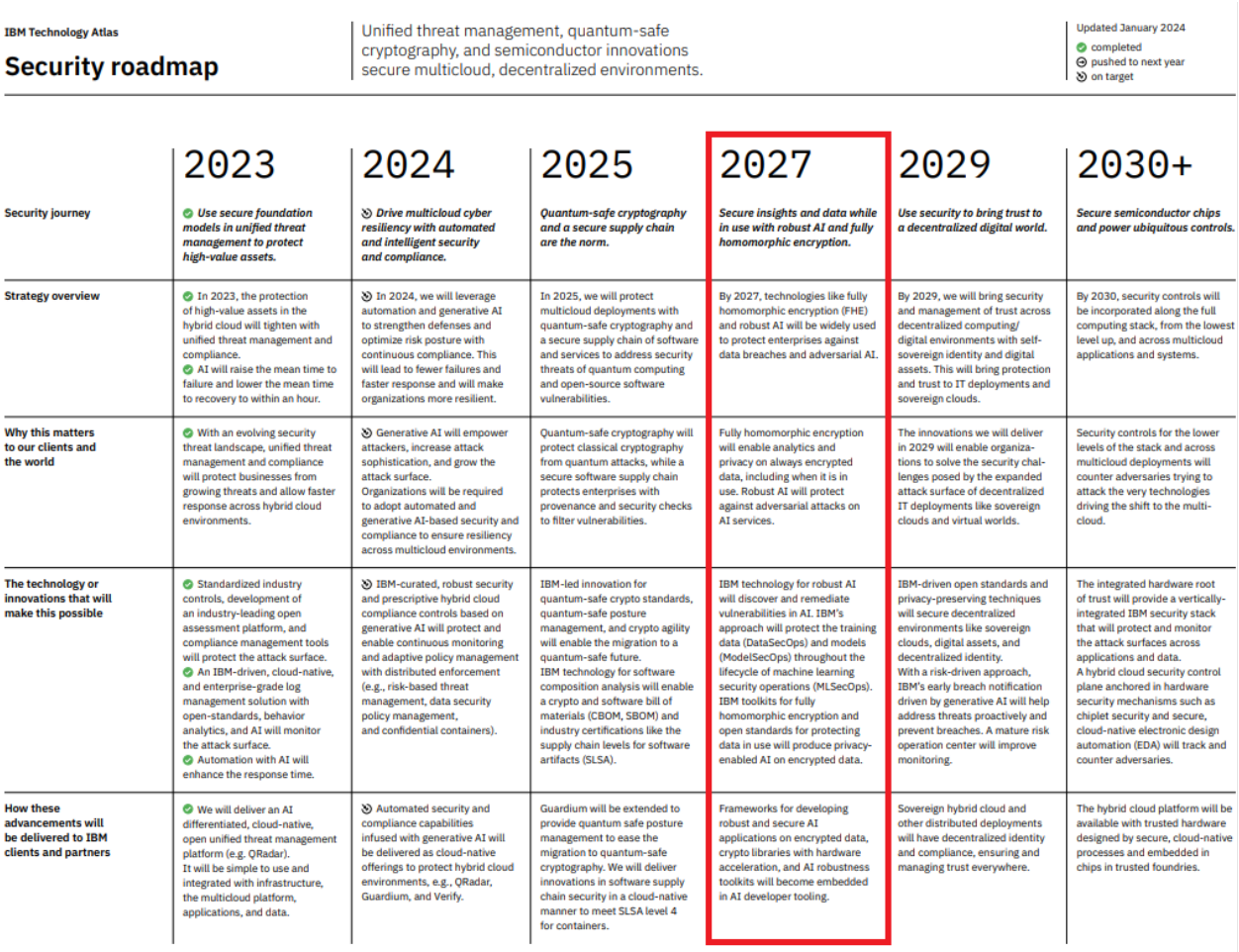
Contribuição (300 caracteres): Com objetivo de introduzir o tema à sociedade e ao leitor, o presente estudo poderia mencionar questões relacionadas ao uso da criptografia homomórfica, que permite trabalhar com dados criptografados sem a necessidade de descriptografá-los, minimizando a possibilidade de exposição das informações.

Considerações:

Como exemplo, temos a utilização da criptografia homomórfica para análises preditivas em serviços financeiros, uma vez que permite o cálculo de dados criptografados com modelos de machine learning sem expor as informações; pesquisas de comportamento de consumidores, auxiliando a obter informações sobre o comportamento do consumidor, ocultando as consultas dos usuários e protegendo o direito à privacidade do indivíduo. (Disponível em: https://www.ibm.com/topics/homomorphic-encryption. Acesso em: 26/02/2024).

Além disso, o Security Roadmap publicado pela IBM, estabelece que até 2027 a criptografia homomórfica será amplamente utilizada para proteger as empresas

contra violações de dados, pois permitirá a análise e a privacidade em dados sempre criptografados, inclusive quando eles estão em uso. Disponível em: https://www.ibm.com/roadmaps/security.pdf. Acesso em: 26/02/2024).



IBM Technology Atlas

Security roadmap

Unified threat management, quantum-safe cryptography, and semiconductor innovations secure multicloud, decentralized environments.

Updated January 2024
completed
pushed to next year
on target

	2023	2024	2025	2027	2029	2030+
Security journey	***Use secure foundation models in unified threat management to protect high-value assets.***	***Drive multicloud cyber resiliency with automated and intelligent security and compliance.***	***Quantum-safe cryptography and a secure supply chain are the norm.***	***Secure insights and data while in use with robust AI and fully homomorphic encryption.***	***Use security to bring trust to a decentralized digital world.***	***Secure semiconductor chips and power ubiquitous controls.***
Strategy overview	In 2023, the protection of high-value assets in the hybrid cloud will tighten with unified threat management and compliance. AI will raise the mean time to failure and lower the mean time to recovery to within an hour.	In 2024, we will leverage automation and generative AI to strengthen defenses and optimize risk posture with continuous compliance. This will lead to fewer failures and faster response and will make organizations more resilient.	In 2025, we will protect multicloud deployments with quantum-safe cryptography and a secure supply chain of software and services to address security threats of quantum computing and open-source software vulnerabilities.	By 2027, technologies like fully homomorphic encryption (FHE) and robust AI will be widely used to protect enterprises against data breaches and adversarial AI.	By 2029, we will bring security and management of trust across decentralized computing/ digital environments with self-sovereign identity and digital assets. This will bring protection and trust to IT deployments and sovereign clouds.	By 2030, security controls will be incorporated along the full computing stack, from the lowest level up, and across multicloud applications and systems.
Why this matters to our clients and the world	With an evolving security threat landscape, unified threat management and compliance will protect businesses from growing threats and allow faster response across hybrid cloud environments.	Generative AI will empower attackers, increase attack sophistication, and grow the attack surface. Organizations will be required to adopt automated and generative AI-based security and compliance to ensure resiliency across multicloud environments.	Quantum-safe cryptography will protect classical cryptography from quantum attacks, while a secure software supply chain protects enterprises with provenance and security checks to filter vulnerabilities.	Fully homomorphic encryption will enable analytics and privacy on always encrypted data, including when it is in use. Robust AI will protect against adversarial attacks on AI services.	The innovations we will deliver in 2029 will enable organizations to solve the security challenges posed by the expanded attack surface of decentralized IT deployments like sovereign clouds and virtual worlds.	Security controls for the lower levels of the stack and across multicloud deployments will counter adversaries trying to attack the very technologies driving the shift to the multi-cloud.
The technology or innovations that will make this possible	Standardized industry controls, development of an industry-leading open assessment platform, and compliance management tools will protect the attack surface. An IBM-driven, cloud-native, and enterprise-grade log management solution with open-standards, behavior analytics, and AI will monitor the attack surface. Automation with AI will enhance the response time.	IBM-curated, robust security and prescriptive hybrid cloud compliance controls based on generative AI will protect and enable continuous monitoring and adaptive policy management with distributed enforcement (e.g., risk-based threat management, data security policy management, and confidential containers).	IBM-led innovation for quantum-safe crypto standards, quantum-safe posture management, and crypto agility will enable the migration to a quantum-safe future. IBM technology for software composition analysis will enable a crypto and software bill of materials (CBOM, SBOM) and industry certifications like the supply chain levels for software artifacts (SLSA).	IBM technology for robust AI will discover and remediate vulnerabilities in AI. IBM's approach will protect the training data (DataSecOps) and models (ModelSecOps) throughout the lifecycle of machine learning security operations (MLSecOps). IBM toolkits for fully homomorphic encryption and open standards for protecting data in use will produce privacy-enabled AI on encrypted data.	IBM-driven open standards and privacy-preserving techniques will secure decentralized environments like sovereign clouds, digital assets, and decentralized identity. With a risk-driven approach, IBM's early breach notification driven by generative AI will help address threats proactively and prevent breaches. A mature risk operation center will improve monitoring.	The integrated hardware root of trust will provide a vertically-integrated IBM security stack that will protect and monitor the attack surfaces across applications and data. A hybrid cloud security control plane anchored in hardware security mechanisms such as chiplet security and secure, cloud-native electronic design automation (EDA) will track and counter adversaries.
How these advancements will be delivered to IBM clients and partners	We will deliver an AI differentiated, cloud-native, open unified threat management platform (e.g. QRadar). It will be simple to use and integrated with infrastructure, the multicloud platform, applications, and data.	Automated security and compliance capabilities infused with generative AI will be delivered as cloud-native offerings to protect hybrid cloud environments, e.g., QRadar, Guardium, and Verify.	Guardium will be extended to provide quantum safe posture management to ease the migration to quantum-safe cryptography. We will deliver innovations in software supply chain security in a cloud-native manner to meet SLSA level 4 for containers.	Frameworks for developing robust and secure AI applications on encrypted data, crypto libraries with hardware acceleration, and AI robustness toolkits will become embedded in AI developer tooling.	Sovereign hybrid cloud and other distributed deployments will have decentralized identity and compliance, ensuring and managing trust everywhere.	The hybrid cloud platform will be available with trusted hardware designed by secure, cloud-native processes and embedded in chips in trusted foundries.

B/LUZ
R. Ramos Batista. 444. Vila Olímpia
04552-020. São Paulo – SP
baptistaluz.com.br

/ Ref.: **Contribuição – Consulta Pública – Estudo Preliminar – Anonimização e Pseudonimização para Proteção de Dados Pessoais ("Guia")**

/ Para: **Autoridade Nacional de Proteção de Dados ("ANPD")**

/ De: **b/luz**

/ Data: 14 de março de 2024

Subitem 2.2 – parágrafo 18

1. Título

Necessidade de pronunciamento da Autoridade Nacional de Proteção de Dados a respeito da interpretação dada ao art. 12, § 2º, da LGPD.

2. Sugestão

O art. 12, § 2º, da LGPD considera igualmente dados pessoais aqueles utilizados para a formação do perfil comportamental de determinada pessoa natural, se identificada. Apesar da redação intrincada do dispositivo, uma interpretação provável, segundo determinados autores, é a de que a LGPD se aplicaria mesmo a dados anonimizados nas circunstâncias em que houver formação de perfil comportamental do titular dos dados pelo controlador. Com isso, parece, a intenção é expandir o regime protetivo da LGPD às situações nas quais o uso de dados anonimizados impacte os direitos e as liberdades fundamentais do titular, especialmente, nesse dispositivo, para a formação de perfis comportamentais. Por outro lado, o parágrafo aparenta contradizer-se ao incluir, *in fine*, a expressão "se identificada" – o que denota um vício lógico e possível redundância, uma vez que, se o titular já é identificado, caracteriza-se, invariavelmente, um dado pessoal.

Diante das divergências interpretativas frente ao dispositivo, sugere-se que a ANPD se pronuncie a respeito da interpretação dada ao art. 12, § 2º, da LGPD a fim de reduzir a insegurança relativa ao tema.

Subitem 3.1.1 – parágrafos 34 ao 36

3. Título

Reconhecimento da compatibilidade do procedimento de anonimização com as finalidades iniciais de tratamento, abarcando a hipótese de término do tratamento de dados do art. 16, IV, da LGPD.

4. Sugestão

No parágrafo 34, afirma-se que o controlador deve informar com clareza quando uma das finalidades da coleta dos dados pessoais for a futura anonimização. Caso contrário, o procedimento de anonimização importará tratamento posterior ou uso secundário, que deverá ser compatível com a finalidade inicialmente informada. Essa afirmação parte da premissa de que o procedimento de anonimização é uma espécie de tratamento de dados, sujeitando-se à aplicação integral das regras e princípios da LGPD, até mesmo após a anonimização completa.

Ocorre que, ao mesmo tempo, a LGPD determina a eliminação dos dados após o término do tratamento (art. 16) – ou, alternativamente, permite a anonimização para uso exclusivo do controlador (art. 16, IV). Essa permissão implica um reconhecimento de que o procedimento de anonimização é, *a priori*, compatível com o princípio da adequação e da finalidade previstos na LGPD, afinal, o objetivo do procedimento de anonimização é justamente o término do tratamento e a quebra do vínculo de identificação com o titular dos dados – o que se coaduna, além disso, com o princípio da necessidade.

É improvável, portanto, uma situação na qual o procedimento de anonimização seja incompatível com uma finalidade inicialmente informada – salvo se ilícita – uma vez que a própria lei incentiva os controladores a anonimizarem os dados e a anonimização resulta numa redução do risco para o titular. Na União Europeia, o *Working Party 29* reconheceu explicitamente que o procedimento de anonimização é compatível com as finalidades iniciais de tratamento, desde que realizado de maneira adequada.[1]

Sugere-se, portanto, que o parágrafo 34 e seguintes sejam reformulados para que seja **reconhecida a compatibilidade do procedimento de anonimização com tratamentos anteriores**, em linha, aliás, com o que dispõem os parágrafos 39 e 54.

***

[1] "Accordingly, the Working Party considers that anonymisation as an instance of further processing of personal data can be considered to be compatible with the original purposes of the processing but only on condition the anonymisation process is such as to reliably produce anonymised information in the sense described in this paper". ARTICLE 29 DATA PROTECTION WORKING PARTY. **Opinion 05/2014 on Anonymisation Techniques**, p. 07. Bruxelas: [s. n.], 2014. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. Acesso em 22 de fev. de 2024.

Subitem 3.1.3 – parágrafo 52

1. Título

Supressão de trecho do parágrafo tendo em vista a não abrangência do termo "outras pessoas ou entidades" na caracterização dos "meios próprios" descritos no art. 12 da LGPD.

2. Sugestão

O parágrafo 52 afirma: "*Sendo assim, importa ressaltar que, a partir do art. 12, 'caput', da LGPD, compreende-se que a avaliação da possibilidade de reidentificação de dados e a reversão do processo de anonimização devem ter em consideração não apenas o uso de meios próprios do agente de tratamento responsável pela anonimização, mas também a atuação de outras pessoas ou entidades que, com meios e esforços razoáveis, podem reidentificar [o] conjunto de dados anonimizados*".

A expressão "outras pessoas ou entidades" é uma provável referência ao Considerando n. 26[2] do Regulamento n. 2016/679 da União Europeia. Essa referência, contudo, não encontra correspondência na LGPD. Pelo contrário, no texto normativo do art. 12 da LGPD, o termo "meios próprios" é modificado pelo advérbio "exclusivamente", o que parece refletir uma escolha do legislador para restringir os meios próprios apenas a aqueles disponíveis ao controlador na ocasião do tratamento, assim excluindo outras pessoas, entidades e demais terceiros que se relacionem com o agente de tratamento.

Apesar disso, a inteligência do parágrafo 52 afirma o contrário, tirando por conclusão que, diante do art. 12 da LGPD, os meios próprios deveriam também abranger a atuação de outras pessoas ou entidades, sem, contudo, pormenorizar o raciocínio jurídico que resultou dessa conclusão.

Diante disso, sugere-se a **supressão do trecho do parágrafo 52 destacado acima**.

***

[2] "The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. **To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly.** To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes." (g. n.)

Subitem 3.2 – parágrafos 70 - 75

1. Título

Inclusão de exemplos e maiores explicações.

2. Sugestão

Em que pese o fato de o Guia destacar a impossibilidade de estabelecer uma métrica única para a mensuração do risco real de reidentificação, seria importante que o Guia buscasse aprofundar nas métricas sugeridas, enriquecendo com mais exemplos e casos que tornem mais concreta a proposta descrita na "Figura 2: Processo de anonimização baseado em risco".

Além disso, o Guia poderia adicionar elementos ou situações diversas que envolvam, por exemplo, outras categorias de dados pessoais, tipos de titular, atividades de tratamento de dados pessoais, entre outras situações, que possam ajudar no entendimento da aplicação dos conceitos de Valor Geral da Métrica Contextual (θ) e Fator de Ponderação das Variáveis Contextuais (Vc) para avaliação do Risco de Reidentificação Mensurado ("RRM").

3. Referência

CAVOUKIAN, Ann; EMAM, Khaled El. **Protecting Privacy Using k-Anonymity**, 2008. Disponível em: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2528029/ . Acesso em: 20 fev. 2024.

***

Subitem 3.3 – parágrafo 84

1. Título

Reformulação da metodologia eficaz de pseudonimização.

2. Sugestão

A proposta de metodologia apresentada pode encontrar dificuldades de implementação por misturar etapas gerais com etapas específicas do processo de aplicação da metodologia de pseudonimização. Por exemplo, a etapa "Desenvolvimento de Políticas e Procedimentos" está dentro de um fluxo macro responsável por reger todos os processos de "Avaliação Inicial e Identificação dos Dados Objeto da Pseudonimização" e, portanto, deveria ser uma etapa antecessora.

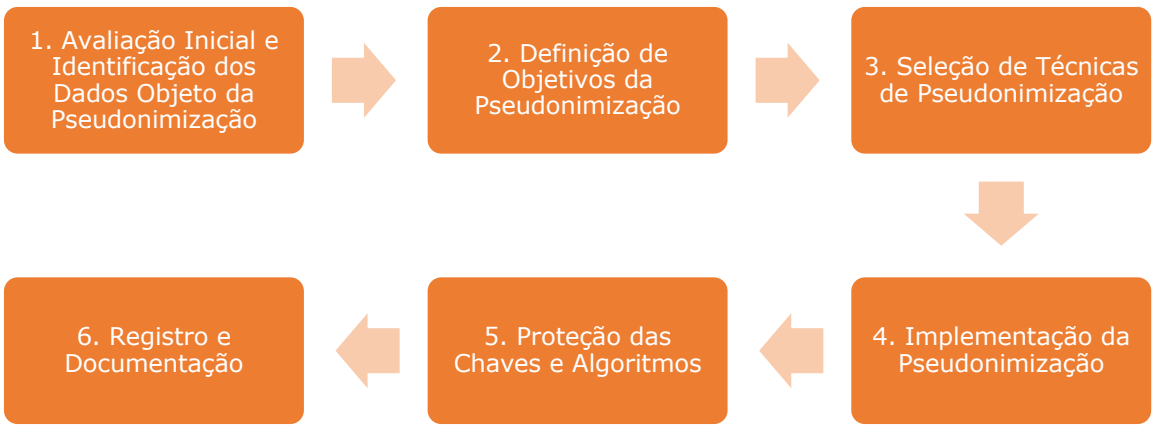
Diante dessa observação, propomos a separação da metodologia em dois fluxos, um macro e outro específico, conforme a sugestão abaixo.

Macro:

Notem que todas as etapas indicadas acima se comportam como pressupostos básicos e gerais para que o processo de pseudonimização das atividades pelo agente de tratamento de fato ocorra de forma adequada e alinhada às expectativas definidas pelo próprio agente de tratamento.

Superada as etapas descritas no fluxo macro, deve-se iniciar um fluxo específico, previamente descrito na Política ou Procedimento, que irá reger como o agente de tratamento irá aplicar a metodologia de pseudonimização no caso concreto.

Específico:



Vale ressaltar que as últimas três etapas previstas no fluxo original da "Figura 3: Metodologia Eficaz de Pseudonimização" foram suprimidas, conforme as justificativas abaixo:

- **Avaliação de Impacto à Proteção de Dados:** A recomendação de aplicação do RIPD apenas para avaliar os riscos associados à pseudonimização não se mostra um meio de avaliação adequado, tendo em vista que seu propósito normativo de avaliação é de escopo mais amplo e dedicado à descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais. Portanto, sugerimos sua total supressão, ou a adaptação do texto para indicar que a avaliação da metodologia de pseudonimização deve ser considerada como um elemento, dentre outros, a serem analisados para mitigação dos riscos associados ao processo em análise no RIPD.

- **Comunicação com os Titulares:** A necessidade de transparência é um pressuposto básico para todas as atividades de tratamento de dados pessoais. Contudo, no caso específico da pseudonimização, essa etapa proposta no Guia não se mostra muito clara em termos concretos de aplicação, não deixando claro se deve ser divulgada a técnica aplicada. Ademais, as metodologias de pseudonimização podem ser demasiadamente complexas para serem compreendidas pelo público geral, o que comprometeria o objetivo de garantir uma comunicação transparente com os titulares dos dados. Diante dessas razões, sugerimos a remoção dessa etapa.

- **Plano de Resposta a Incidentes de Segurança:** Trata-se de um processo geral que deve cobrir todas e quaisquer atividades de tratamento, independentemente da aplicação da metodologia de pseudonimização. Portanto, sua inclusão específica dentro da metodologia de pseudonimização gera uma redundância desnecessária.

***

Subitem 3.3 – parágrafo 84

1. Título

Inclusão de uma metodologia de pseudonimização adequada a agentes de tratamento de pequeno porte.

2. Sugestão

A metodologia de pseudonimização apresentada no Guia se mostra demasiadamente sofisticada, dependendo, em vários momentos, de recursos técnicos e do apoio de profissionais especializados que podem representar, na prática, em um desincentivo financeiro para sua implementação por agentes de tratamento de pequeno porte, diante do benefício da supressão do risco mapeado.

Portanto, a fim de transformar o Guia em um documento de incentivo à implementação das técnicas de anonimização e pseudonimização, sugerimos que as etapas que possam representar um alto custo de gestão e implementação (como, por exemplo, as etapas (i) Monitoramento e Auditoria; e (ii) Registro e Documentação descritas na "Figura 3: Metodologia Eficaz de Pseudonimização") sejam simplificadas para agentes de tratamento de pequeno porte.

***

Apêndice II. Caderno de Técnicas para Anonimização e Pseudonimização

1. Título

Revisão crítica dos exemplos apresentados

2. Sugestão

As técnicas de anonimização ilustradas de forma exemplificativa são importantes para uma melhor compreensão, porém necessitam de revisão para evitar confusões em sua aplicação por parte dos agentes de tratamento. Por exemplo, no caso das ilustrações que demonstram como a técnica de anonimização de imagem deve ser aplicada, o Guia dá a entender que o desfoque ou pixelização dos olhos do indivíduo é suficiente para anonimizar a imagem. Tal sugestão, como pode ser observado no Guia, preserva diversos traços da face do titular, aumentando significativamente o risco de reidentificação. Portanto, sugerimos que a imagem proposta seja revisada para ilustrar situações que demonstram ter um menor de risco de reidentificação do titular, conforme o exemplo abaixo:

4. Referência

INFORMATION COMISSIONER'S OFFICE. **Anonymisation: managing data protection risk code of practice**, 2012. Disponível em: https://ico.org.uk/media/1061/anonymisation-code.pdf. Acesso em: 20 fev. 2024.

***

Apêndice IV. Estudo de Casos

1. Título

Revisão crítica do Caso 3

2. Sugestão

Conforme pode ser observado na "Tabela 9: Risco Reidentificação", o identificador "matrícula", avaliado pelo critério de K-Anonimização, em alguns momentos ficou muito acima do RRA esperado (0,35), conforme destacado na tabela abaixo:

Identificador	K-Anonimização por Classe do Identificador	K-Anonimização do Identificador (Média da K-Anonimização por Classe do Identificador)
Matrícula	**2301* = 12 =0,50 **2302* = 13 = 0,33 **2303* = 14 = 0,25 **2304* = 11 = 1,00	0,52

Para estas situações, apesar do resultado da Métrica Contextual do caso analisado ser positivo (0,31), ou seja, menor que o RRA esperado, a capacidade de reidentificação pela matrícula é alta. Em especial, para o caso em que o resultado apurado por classe do identificador foi "1,00" (matrícula **2304*), a capacidade de reidentificação é máxima.

Sendo assim, mostra-se relevante considerar o estabelecimento de parâmetros mais granulares para a definição da métrica contextual (nesse caso em específico, por classe do identificador), a fim de chamar a atenção para casos que podem ser capazes de comprometer parcialmente ou totalmente a base anonimizada.

Sendo assim, sugerimos que seja considerada a aplicação de uma Métrica Contextual por classe do identificador, a fim de expurgar qualquer indentificador sobressalente capaz de comprometer a base anonimizada.

***

São Paulo, 13 de março de 2024.

À Autoridade Nacional de Proteção de Dados ("ANPD")

Ref.: Estudo Preliminar sobre Anonimização e Pseudonimização para proteção de dados pessoais

Prezados Senhores,

A Associação das Empresas de Tecnologia da Informação e Comunicação e Tecnologias Digitais ("BRASSCOM"), é entidade sem fins lucrativos de representatividade nacional, e que congrega algumas das mais dinâmicas e inovadoras empresas de TIC alinhadas com a Transformação Digital do Brasil.

De início, louvamos a ANPD pela apresentação deste Estudo Preliminar ("Estudo"), o qual elucida pontos importantes acerca das técnicas de anonimização e pseudonimização para proteção dos dados pessoais. Consideramos fundamental essa iniciativa de abrir espaço para que todas as partes interessadas possam apresentar considerações, e permitir que a normatização em torno da Lei Geral de Proteção de Dados Pessoais ("LGPD") atinja os seus objetivos de forma equilibrada e eficiente.

Sempre com o intuito de enriquecer o debate e contribuir na melhoria do endereçamento no tema, a Brasscom, respeitosamente, compartilha as considerações das indústrias da tecnologia, conforme seguem:

1. Das definições

Conforme indica a ANPD no item 2 do Estudo Preliminar[1], para a melhor compreensão das orientações que se pretende passar, se faz importante esclarecer o significado de alguns termos empregados ao longo do documento. Em primeiro lugar, embora se entenda o objetivo da inclusão de um glossário específico para cada documento produzido por essa autoridade, seria interessante que as referências sejam sempre feitas

[1] Página 5 do Estudo Preliminar sob consulta.

ao Glossário de Proteção de Dados Pessoais e Privacidade[2], a fim de que se mantenha a uniformização e padronização de termos comuns, ao invés de um mesmo termo ser empregado diferentemente a depender do contexto ou documento.

1.1. Dado Pseudonimizado

Não obstante a consideração acima feita, a Brasscom entende que o conceito de dado pseudonimizado precisa de correção.

Isso porque, em diversos itens do Estudo Preliminar da ANPD, compreende-se que o procedimento de pseudonimização requer que a informação capaz de reverter o processo esteja sob posse do "controlador". Em outras palavras, a reversão só é possível por meio do uso de informações adicionais mantidas separadamente pelo controlador. No entanto, é relevante destacar que o operador também pode conduzir integralmente o processo de pseudonimização, mantendo a informação reversora de forma segura em seu próprio ambiente. A interpretação do processo de pseudonimização sendo direcionada apenas ao controlador, embora prevista no artigo 13 §4º da LGPD, conflita com o objetivo e espírito da Lei, que incentiva a adoção de técnicas de segurança em dispositivos.

Deste modo, é imperativo que a ANPD esclareça a interpretação extensiva do artigo 13 §4º da LGPD, pois em um cenário em que o operador trata, em nome do controlador, diversos dados de identificação direta e indireta e aplica internamente técnicas de pseudonimização, isolando em seu próprio ambiente, os dados que permitiriam a identificação do titular, haveria uma lacuna na compreensão do processo aplicado pelo operador se se configuraria igualmente como pseudonimização, já que a informação adicional que permitiria a associação direta ou indireta a um indivíduo está no ambiente do próprio operador e não do controlador, como disposto na Lei e no Estudo Preliminar. Assim, onde lê-se "controlador" no art. 13 §4º, deveria ler-se "agente de tratamento", cabendo à ANPD trazer esse esclarecimento.

[2] Autoridade Nacional de Proteção de Dados. Glossário de Proteção de Dados Pessoais e Privacidade. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/glossario-anpd-protecao-de-dados-pessoais-e-privacidade.pdf

2. Dos contornos do dado anonimizado

A definição de dado anonimizado consta da própria LGPD, em que estabeleceu ser o dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. Em outras palavras, o dado anonimizado é o *output* da aplicação de medidas técnicas de anonimização ou, conforme esclarece a ANPD, o resultado do processo de remoção dos identificadores diretos e indiretos que estabeleciam o caráter pessoal do dado[3]. Sendo, portanto, a identificabilidade um elemento central para avaliar se tratar ou não de um dado pessoal, a LGPD estabeleceu critérios que devem ser considerados na avaliação da robustez da técnica de anonimização empregada e dos riscos de reidentificação do dado: os esforços razoáveis e os meios próprios[4].

1.1 Esforços razoáveis e meios próprios

Ao analisar os dois termos previstos na LGPD, a ANPD estabeleceu que o conceito de "esforços razoáveis" configura um conceito jurídico indeterminado, pelo que compete à ANPD, como intérprete e aplicadora, por excelência, da LGPD, avaliá-lo contextualmente. Além disso, indicou que o rol apresentado no parágrafo primeiro do artigo 12 é exemplificativo, indicando alguns dos aspectos objetivos para avaliar, no caso concreto, o conceito de esforços razoáveis.

No entanto, a Autoridade finaliza pontuando que a leitura do *caput* do artigo 12 leva à conclusão de que a avaliação da possibilidade de reidentificação de dados e a reversão do processo de anonimização devem ter em consideração *não apenas o uso de meios próprios do agente de tratamento responsável pela anonimização, mas também a atuação de outras pessoas ou entidades* que, com meios e esforços razoáveis, podem reidentificar conjunto de dados anonimizados. Neste ponto, nos parece que a interpretação está demasiadamente extensiva, ou carece de contextualização.

Vale destacar que, diferentemente do GDPR que, expressamente previu que *para determinar se o dado pode ser considerado pessoal, deverão ser tidos em conta todos*

[3] Página 7 do Estudo Preliminar sob consulta.
[4] V. Art. 12, LGPD.

os meios razoavelmente susceptíveis de serem utilizados, quer pelo responsável pelo tratamento, quer por outra pessoa[5], a LGPD assim não o fez, tendo empregado de forma repetida, no *caput* e parágrafo primeiro do Artigo 12, *a utilização exclusiva de meios próprios*. Ainda que a ANPD possa considerar, os esforços razoáveis de terceiros na análise contextual, a conclusão deve ser modificada.

1.2 Dados Anonimizados sob a perspectiva do destinatário dos dados

Um outro ponto que deve ser mais explorado pela ANPD refere-se a análise subjetiva do dado anonimizado ou pseudonimizado compartilhado, sob a perspectiva do controlador (remetente) e da parte receptora dos dados. Nesse sentido, vale a pena citar recente julgado da Corte Geral da União Europeia[6], em que se estabeleceu o quanto segue:

(i) Citando julgado paradigma da Corte de Justiça da União Europeia, reforçou que o fato de as informações adicionais necessárias para identificar os titulares de dados não terem sido compartilhadas com o receptor dos dados, não seria, *a priori*, suficientes para afastar a identificabilidade dos dados;

(ii) É necessário colocar-se na posição do receptor dos dados, para determinar se as informações que lhe são transmitidas dizem respeito a pessoas identificáveis;

---

[5] Redação original: *The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.* Recital 26 da GDPR. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679

[6] Judgment of the General Court. Case T-557/20. Disponível em: https://curia.europa.eu/juris/document/document.jsf?text=&docid=272910&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1900702

(iii) A análise, sob a perspectiva do receptor, deve considerar se ele dispunha de meios legais que lhe pudessem, na prática, ter acesso às informações adicionais necessárias para reidentificar os titulares.

Ou seja, a divulgação de um conjunto de dados pseudonimizados pelo controlador, sem os identificadores separados, consiste, *a priori,* no compartilhamento de base de dados anonimizada do ponto de vista do destinatário[7]. Embora essa conclusão possa ser inferida do Estudo de Caso incluído como apêndice ao Estudo Preliminar, seria importante que a ANPD incluísse no próprio estudo, uma análise da anonimização e da pseudonimização sob a perspectiva dos destinatários dos dados.

1.3 Da reidentificação dos dados

A Brasscom parabeniza a ANPD pela abordagem flexível dada ao processo de anonimização, que afasta o conceito binário da anonimização, prestigiando, dessa forma, a escolha dos agentes de tratamento na metodologia e técnica que melhor se adeque às suas atividades, levando em conta aspectos contextuais do tratamento e o grau de utilidade do dado. É também uníssono que uma efetiva anonimização, no presente, não afasta completamente os riscos de reversão da anonimização no futuro, especialmente considerando o constante aprimoramento e desenvolvimento de novas tecnologias.

Contudo, é importante que se esclareça que, quando se constatar, durante o processo de gestão de riscos de reidentificação, que as condições antes indicativas de uma efetiva anonimização não estão mais sendo mais atendidas, não se deve pressupor um tratamento anterior ilícito[8], dada a impossibilidade de a lei retroagir em prejuízo do

[7] ICO, Introduction to anonymisation. Draft anonymisation, pseudonymisation and privacy enhancing technologies guidance, página 9: "In the ICO's view, the same information can be personal data to one organisation, but anonymous information in the hands of another organisation. Its status depends greatly on its circumstances, both from your perspective and in the context of its disclosure." Disponível em: https://ico.org.uk/media/about-the-ico/consultations/2619862/anonymisation-intro-and-first-chapter.pdf

[8] Em outras palavras, se todo tratamento de dado pessoal deve ser legitimado por ter suporte normativo em hipótese legal estabelecida previamente, como as previstas nos artigos 7º e 11 da LGPD, a anonimização pressupõe tratamento lícito, pois não é processo capaz de transformar em legítima a irregular atividade de tratamento de dados sem fundamentação legal. Parágrafo 31 do Estudo Preliminar sob consulta.

controlador. Nesse caso, sugere-se esclarecer a ANPD, caberá ao controlador: (i) reiniciar o processo de anonimização; ou (ii) proceder com a exclusão dos dados.

Em outro ponto, seria importante que a ANPD esclarecesse as consequências jurídicas, afastando a responsabilidade do controlador, quando a reindentificação ocorrer por ato ilegítimo e ilegal de terceiros, isso pois, fazendo referência ao direito comparado, para avaliação de um risco de desanomização por um terceiro, deve-se levar em consideração os meios "legais" que tal terceiro poderá empregar para obter dados auxiliares e assim, ter acesso ao dado pessoal.[9]

2. Anonimização como processo acessório ao tratamento de dados pessoais

Entende-se a anonimização como um processo acessório ao tratamento de dados pessoais propriamente dito, que tem por objetivo, como antes dito, desassociar identificadores diretos ou indiretos presentes no dado pessoal, com a aplicação de medidas técnicas de segurança. Nessa linha, parece razoável que a aplicação dos princípios e regras de proteção de dados mencionadas pela ANPD no parágrafo 32 do seu Estudo Preliminar se refira a uma análise global do tratamento de dados e não, de forma individualizada, para o processo de anonimização. A anonimização não é uma finalidade em si mesma a ponto de o "processo de anonimização" ser considerado uma operação de tratamento de dados. Pensar diferente é esvaziar o tratamento de dados de sua finalidade subjacente, embora primordial, sugerindo que cada medida técnica aplicada para a proteção de dados pessoais seja individualizada a um tratamento de dados *per se.*

Corroborando o entendimento acima, podemos citar os artigos 5º, inciso IV e artigo 11, inciso, II, alínea b, da LGPD que ao possibilitar o tratamento de dados para a realização de estudos por órgão de pesquisa, recomenda, sempre que possível, que o controlador dos dados garanta a anonimização dos dados. Note-se que o texto legal

[9] Case T-557/20. Disponível em: https://curia.europa.eu/juris/document/document.jsf?text=&docid=272910&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2176772

segrega a finalidade do tratamento (relacionada aos estudos do órgão de pesquisa) da medida de proteção a ser aplicada, quando possível (a anonimização).

Há de se mencionar ainda, o artigo 18 que indica a anonimização como direito alternativo ao bloqueio e exclusão de dados, quando do tratamento de dados excessivos ou em desconformidade com a LGPD. O que, uma vez mais, demonstra ser a anonimização uma atividade acessória, que garante o cumprimento dos princípios da segurança, prevenção e prestação de contas, do artigo 46 da LGPD (Segurança e Sigilo dos dados), e até mesmo o término do tratamento de dados pessoais (conforme abaixo melhor se abordará). Assim sendo, não se caracteriza como uma atividade autônoma de tratamento de dados pessoais. Isso é reforçado, inclusive, pela redação do *caput* artigo 13 da LGPD[10] que expressamente coloca a anonimização e pseudonimização como "práticas de segurança" empregadas aos dados pessoais.

Deve-se pontuar, por fim, que a anonimização, *per se*, já se alinha aos princípios da LGPD, na medida em que assegura que apenas os dados pessoais necessários e adequados para os propósitos específicos sejam conservados, já que os dados anonimizados, vale novamente mencionar, não mantém elementos informativos relacionados à pessoa identificada ou identificável. Logo, é importante a ANPD esclarecer que a anonimização não é uma finalidade em si mesma a ponto de o "processo de anonimização" ser considerado uma operação de tratamento de dados.

4. Da exigência da compatibilidade entre o processo de anonimização de dados e a finalidade inicial da coleta

Embora a Brasscom entenda que o processo de anonimização é acessório às operações de tratamento propriamente ditas e com elas não se confunde, caso a ANPD entenda por rejeitar tal premissa, passa-se a discorrer sobre o processo de anonimização nos termos trazidos pelo Estudo Preliminar.

[10] *"Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a 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".* (grifos nossos)

A ANPD, no item 35 do Estudo Preliminar, dispõe que caso a finalidade de anonimização não tenha sido informada originalmente, a sua realização importará "tratamento posterior" ou uso secundário que, necessariamente, deverá ser compatível com a finalidade inicialmente informada.

Com relação ao acima disposto, entendemos que a determinação de que o tratamento dos dados anonimizados importará em "finalidade secundária" não faz muito sentido, na medida em que a anonimização dos dados pessoais deve ser estimulada. Caso seja necessário (i) exigir tal compatibilidade, ou exigir a (ii) renovação da informação ao agente sobre a possível anonimização dos seus dados, caso a finalidade seja supostamente incompatível, a ausência de informação impedirá a anonimização, o que conflita com o espírito da LGPD.

Ademais, com a anonimização, o dado deixa de ser considerado dado pessoal, o que afasta a aplicabilidade da LGPD após o processo de anonimização. Portanto, qual a utilidade em informar ao titular sobre a anonimização se ele deixará de ser um dado pessoal e a LGPD não mais incidirá?

Deste modo a Brasscom entende que a citada compatibilidade não deve ser exigida. O que na verdade deve ser entendido e poderia constar no Estudo Preliminar é que todo e qualquer dado pessoal pode ser anonimizado se assim decidir o controlador de dados, especialmente em virtude do que dispõe o artigo 16 IV da LGPD.

5. Conservação de dados anonimizados após o término do tratamento de dados

A Brasscom se preocupa com a conclusão apontada pela ANPD no parágrafo 39 do Estudo Preliminar, em que se menciona que atingida a finalidade do tratamento de dados, a conservação dos dados, para uso exclusivo do controlador, será permitida, *desde que, à luz do princípio da necessidade, os dados sejam anonimizados.* A colocação, no entanto, parece não levar em consideração o artigo 16, inciso IV da LGPD que estabeleceu uma exceção à regra da eliminação, conforme se observa:

> *Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades: (...)*
> *IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.*

A regra é a eliminação dos dados pessoais, tendo sido possibilitada a conservação dos dados anonimizados, por se reconhecer o valor intrínseco de tais dados como insumo para o desenvolvimento econômico e tecnológico.

A decisão do legislador de permitir a conservação de dados anonimizados pelo controlador, para seu uso exclusivo, reflete um esforço consciente para equilibrar os interesses dos titulares dos dados, com a necessidade de estimular a inovação e o desenvolvimento de novos negócios, indo ao encontro com os fundamentos da LGPD[11]. Dessa forma, considerando ser, o artigo 16, IV da LGPD estabeleceu uma derrogação às regras gerais de eliminação desde que os dados sejam anonimizados, ainda que se deva proceder com a gestão dos riscos de reidentificação tratados neste Estudo Preliminar, a manutenção dos dados não deverá estar condicionada ao princípio da necessidade, conforme sugerido pela ANPD, o que se espera seja esclarecido por esta r. Autoridade.

6. Processo de anonimização e intervenção humana

No Apêndice do Estudo Preliminar, item "k", afirma-se que a "anonimização não deve ser totalmente automatizada", e em seguida se assume que "dada a importância do contexto e a avaliação geral do processo, poderá ser necessária a intervenção de um especialista humano". A construção apresentada neste item se apresenta contraditória uma vez que não se sabe se a ANPD quis determinar a necessidade de intervenção humana no processo de anonimização ou se pretendeu deixar a critério do agente de tratamento essa decisão.

[11] LGPD, Art. 2º. "A disciplina da proteção de dados pessoais tem como fundamentos: V - o desenvolvimento econômico e tecnológico e a inovação"

Como a LGPD não exige obrigatoriamente tal intervenção, mas ao contrário, permite, para tanto a utilização de quaisquer "meios técnicos razoáveis e disponíveis na ocasião de seu tratamento" (art. 5º, III), a intervenção humana, por consequência, é uma possibilidade a ser implementada se assim os agentes de tratamento entenderem cabível e segundo sua própria avaliação de risco. Logo, não pode ser tratada como um requisito necessário do processo de anonimização, pelo que se sugere retificação da redação do item "k" para seja mais clara nesse sentido, qual seja, no processo de a anonimização a intervenção humana é facultativa e cabe ao agente de tratamento decidir sobre sua conveniência.

7. Estabelecimento de etapas para o processo de pseudonimização

O Estudo Preliminar dispõe, no item 3.3, etapas que devem ser seguidas para a implementação do processo de pseudonimização, o que inclui a elaboração de políticas, realização de avaliação de impacto à privacidade, auditorias, implementação de plano de resposta a incidentes e procedimento para comunicação com titulares.

Entretanto, as referidas medidas são comumente consideradas ações ínsitas ao programa de governança em privacidade dos agentes de tratamento e justificam-se no contexto das atividades de tratamento de dados pessoais, e não do processo de pseudonimização, o qual deve ser entendido como uma medida de segurança.

Dessa forma, nosso entendimento é de que o item deve ser excluído ou revisto, de forma a torná-lo apenas uma recomendação, e não uma imposição, já que não há relação direta com a pseudonimização.

Diante dos apontamentos acima, a Associação se coloca à inteira disposição para continuar contribuindo com as discussões sobre o tema.

Sendo o que nos cumpria para o momento, renovamos nossos votos de elevada estima e consideração.

Cordialmente,

BRASSCOM

São Paulo, 14 de março de 2024.

À Autoridade Nacional de Proteção de Dados (“ANPD”),
Ref.: Estudo Preliminar – Anonimização e Pseudonimização para a proteção de dados pessoais

Prezados Senhores,
A Câmara Brasileira da Economia Digital (“Câmara-e.net”), vem, respeitosamente, à presença de Vossas Senhorias, expor o quanto segue:

1. Apresentação da Câmara-e.net:

A Câmara-e.net é uma entidade sem fins econômicos, multissetorial, que tem como objetivo promover (i) o desenvolvimento integrado e sustentável da economia digital no Brasil; (ii) a segurança nas transações eletrônicas; (iii) a conscientização da cidadania empresarial em todos os níveis, incentivando a discussão e o intercâmbio de ideias e informações sobre comércio eletrônico; e (iv) a formulação de políticas públicas para a consolidação de marcos regulatórios convergentes e no fomento de negócios entre seus associados.

A associação também capacita indivíduos e organizações públicas e privadas para a geração de negócios digitais de forma legal, segura e sustentável, por exemplo, por meio de debates e palestras sobre planejamento de uma loja virtual de sucesso, logística, meios de pagamento na internet, *marketplace*, marketing digital e vendas online.

Além disso, a Câmara-e.net acompanha procedimentos de regulação da economia digital, em qualquer instância decisória, e deles participa ativamente, em busca de modelos adequados ao País, considerando, para tanto, o melhor equacionamento de seu impacto econômico e social, tanto interno como externo.

Cumprimentamos a Autoridade Nacional de Proteção de Dados pela submissão à consulta pública do Estudo Preliminar *Anonimização e Pseudonimização para proteção de dados*, que tem o mérito de transpor ao tema a regulação por riscos, inclusive

reconhecendo que o processo de anonimização não depende do emprego de meios técnicos em específico nem é completamente irreversível do ponto de vista técnico.

Nesse sentido, é particularmente louvável a apresentação, em concreto, no Apêndice 1, de técnicas que se prestam a garantir a anonimização, – dentre os casos exemplificados, destaca-se a técnica de desfoque gaussiano (*blur*), que garante a um só tempo a plena utilidade aos dados anonimizados e o efetivo afastamento de identificadores pessoais, algo que se mostra relevante sobretudo em contexto de leitura por máquina, elemento essencial no treinamento de soluções de inteligência artificial generativa.

Além disso, é também digno de elogios o fato de que a ANPD apresenta - exemplificativamente - etapas do processo de anonimização que podem ser aplicadas com o emprego de diferentes meios técnicos, sempre objetivando gerir os riscos envolvidos sem a ilusão de anulá-los, o que é positivo tanto para agentes de tratamento, que podem adaptar as indicações da Autoridade às suas práticas em concreto, quanto para titulares de dados pessoais, aos quais se busca garantir a proteção adequada.

Em síntese, o Estudo Preliminar fornece os elementos necessários para o entendimento de que a anonimização, tal qual se afigura no atual estado da tecnologia, já tem grande potencial de ser uma importante forma de garantir a proteção à privacidade e proteção de dados e assim concretizar o cumprimento dos princípios da LGPD, devendo, nesta condição, ser incentivada e não obstada.

Todavia, considerando que ainda há espaço para aperfeiçoamentos pontuais, apresentamos os seguintes comentários para o enriquecimento do referido Estudo Preliminar:

2. Termos e Definições constantes do Glossário

Embora entendamos a importância de definições de termos utilizados pela ANPD neste Estudo Preliminar, de modo que se torne mais compreensível ao público destinatário, a Câmara-e.net chama atenção para o fato de que alguns termos aqui utilizados não constam do Glossário de Proteção de Dados Pessoais e Privacidade[1]. A preocupação

[1] Autoridade Nacional de Proteção de Dados. Glossário de Proteção de Dados Pessoais e Privacidade. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/glossario-anpd-protecao-de-dados-pessoais-e-privacidade.pdf

recai na possível falta de uniformização e padronização de definições, de modo a causar insegurança jurídica ao agente regulado.

Noutro ponto, entende-se desnecessária a inclusão de termos definidos pela própria LGPD. Sugere-se, desse modo, que as definições necessárias ao entendimentos dos documentos produzidos pela ANPD sejam sempre em referência ao Glossário de Proteção de Dados e Privacidade, sendo de fundamental relevância a compreensão de que este é um documento vivo e que pode e deve ser atualizado de tempos em tempos.

3. Da metodologia do processo de anonimização

É importante considerar que poderá haver diferentes graus de discernimento quanto à definição do "Risco de Reidentificação Aceitável" (RRA) estipulado e verificado pelos agentes de tratamento. Como bem observa a ANPD, essa determinação possui uma gama de variáveis dependentes do contexto que devem ser observadas pelo agente de tratamento ("*Variável dependente do contexto: Característica interna do agente de tratamento que pode afetar o cálculo do risco de reidentificação*"), sendo certo que agentes de tratamento distintos podem chegar a resultados diferentes sobre o risco de reidentificação aceitável para os dados tratados.

Nesse sentido, seria relevante que, ao discorrer sobre o processo de anonimização no Estudo (p. 18 e 19), a ANPD expressamente aponte sua adesão a uma abordagem flexível quanto à metodologia ali estabelecida: abrindo margem, para além da sua adaptação "*às necessidades de cada agente de tratamento*", para que estes também adotem outros meios e métodos reconhecidos no mercado, por especialistas, ou por outras Autoridades e organizações ao redor do mundo, sem distinção ou preferência entre os possíveis modelos.

4. Anonimização como processo acessório às operações de tratamento de dados pessoais

No parágrafo 37, o Estudo Preliminar se refere ao "Guia Orientativo – Tratamento de dados pessoais pelo Poder Público", incluindo quando ele trata sobre "a existência de conexão fática ou jurídica entre a finalidade original e os objetivos do processo de anonimização." Porém, a anonimização não é uma finalidade em si mesma, mas uma atividade meio para atingir determinada finalidade. Como se verá adiante, a

anonimização não deve requerer base legal própria, pois está conectada com uma finalidade do tratamento que a precedeu.

Embora a LGPD defina como "tratamento" qualquer "modificação" dos dados pessoais, dentre outras operações, uma interpretação sistemática da LGPD permite compreender que a anonimização é um processo técnico e acessório às operações de tratamento de dados pessoais propriamente ditas, de modo que qualificá-la como uma operação de tratamento *per se* traz inconsistências na aplicação da Lei.

Não é por acaso que a LGPD, no inciso seguinte ao que se refere ao "tratamento", define a "anonimização" como a "utilização de meios técnicos razoáveis" (art. 5º, XI), assim como no artigo 13, de forma expressa, coloca a anonimização e pseudonimização como "práticas de segurança" empregadas aos dados pessoais. Corroborando esse entendimento, os próprios artigos 7º e 11, que tratam das bases legais para dados pessoais e dados pessoais sensíveis, respectivamente, trazem como recomendação ao uso da base legal referente à "realização de estudos por órgão de pesquisa" a sugestão da anonimização sempre que possível. Assim, a anonimização é empregada, pelos próprios dispositivos da LGPD, como uma medida técnica de segurança, cujo objetivo é desassociar identificadores diretos ou indiretos do dado pessoal.

Nessa linha, parece razoável que a aplicação dos princípios e regras de proteção de dados mencionadas pela ANPD no parágrafo 32 e seguintes do seu Estudo Preliminar se refira à análise da operação de tratamento principal e não, de forma destacada e individualizada, ao processo de anonimização em si. Até mesmo porque alguns princípios da LGPD terão difícil aplicabilidade nesse contexto.

Exemplifica-se. Pelo princípio da finalidade, o agente de tratamento deveria informar ao titular de dados que uma das finalidades da coleta dos seus dados é a futura anonimização, sendo vedado tratamento posterior de forma incompatível com essa finalidade. No entanto, se a finalidade é a anonimização propriamente dita, eventual "tratamento" posterior escapará à LGPD eis que os dados estarão anonimizados.

Essa incongruência resulta da ausência de observância do art. 12 da LGPD que estipula que o dado anonimizado não será considerado dado pessoal, afastando, portanto, a aplicação da Lei. Logo, **o princípio da finalidade somente seria parcialmente aplicável**: apenas a primeira parte do artigo 6º, inciso I, da LGPD, que trata de "propósitos legítimos", incidirá sobre o ato inicial do processo de anonimização. Com

efeito, o restante do princípio seria aqui inócuo, uma vez que a finalidade em si do banco de dados anonimizados já não está mais regulada pela Lei.

Já pelo princípio da necessidade, um número mínimo de dados pessoais deveria ser tratado, de modo que preferível seria a maximização da anonimização. Outro exemplo de incompatibilidade é o princípio do livre acesso, é dizer: os titulares têm a garantia de consulta facilitada à forma, duração e aos dados pessoais que serão anonimizados? Se os dados foram anonimizados, como será possível aplicar esse princípio?

Essas são apenas algumas das incoerências que são geradas ao se interpretar a anonimização como uma operação de tratamento propriamente dita, bem como ao se exigir análise de compatibilidade, razão pela qual sua natureza jurídica deve ser reconhecida pela ANPD como sendo uma medida de segurança dos dados, afastando do processo de anonimização (i) a necessidade de respaldo por uma base legal, bem como (ii) o monitoramento e a avaliação de finalidades posteriores aplicadas aos dados anonimizados em relação à sua compatibilidade com a finalidade originária.

Cabe destacar que isso não implica, de nenhum modo, menos proteção, cuidado ou cautela no processo de anonimização, tampouco se defende a inaplicabilidade dos princípios e regras da LGPD, os quais certamente devem ser observados na medida do possível, uma vez que há envolvimento de dados pessoais na implementação dessa medida de segurança. O que se pretende, portanto, é a compreensão adequada da natureza do processo de anonimização e que ele possa ser estimulado, não desencorajado pela ANPD.

Não obstante, caso a ANPD entenda de modo diverso ao de que a anonimização é técnica acessória à atividade principal, configurando medida de segurança e proteção aos dados, o que se admite apenas para argumentar, passa-se a discorrer sobre como o processo de anonimização deveria ser compreendido.

4. a. A anonimização não necessita de base legal própria

Em seu parágrafo 30, o Estudo Preliminar afirma que o ato inicial do processo de anonimização se trata de um tratamento de dados pessoais, atraindo assim a aplicação de princípios e regras da LGPD. Adiante, em seu parágrafo 35, ao examinar o princípio da finalidade, o Estudo menciona o conceito de “tratamento posterior”, postulando que,

quando não informada originalmente, a anonimização se trata de um uso secundário e por isso deve ser compatível com a finalidade primeiramente informada.

No caso da operação de anonimização de um dado, tendo em vista o seu objetivo central que é retirar do dado a característica de dado pessoal, não há situação em que tal anonimização possa passar pelo crivo de compatibilidade com a base legal que deu suporte a coleta do dado. Em última análise, trata-se sim de uma medida de segurança para desconfigurar a natureza de pessoal do dado, honrando-se, por via de consequência, inúmeros princípios legais que orientam o tratamento de dados pessoais. Pense-se, por exemplo, numa coleta de dados pessoais inicialmente realizada para a prestação de um serviço – neste cenário, a anonimização posterior dos dados pessoais para análises de eficiência do serviço não apenas é compatível com a finalidade originária, mas garante a preservação da privacidade e dos dados dos usuários e portanto, será sempre uma medida desejada. A partir da anonimização, contudo, os dados deixam de ser regulados pela LGPD, não havendo sentido de análise a respeito das finalidades de atividades de tratamento atreladas ao dado anonimizado.

Deste modo, a anonimização não necessita de base legal própria na medida em que ela sempre será compatível com a finalidade inicial da coleta. Nesse sentido, o Considerando 50 do Regulamento Geral de Proteção de Dados (RGPD) explica que **não há necessidade de base legal própria quando o uso secundário é compatível com o originário**, nos seguintes termos:

> *"The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected.* ***In such a case, no legal basis separate from that which allowed the collection of the personal data is required****."*

Essa linha de raciocínio é especialmente relevante para a anonimização, visto todo o seu potencial para a preservação dos direitos e liberdades fundamentais dos titulares, como demonstrado ao longo do Estudo Preliminar.

Por isso, com o objetivo precípuo de evitar tanto a insegurança jurídica, que poderia advir do silêncio da ANPD sobre a questão, quanto o indevido desestímulo ao uso de técnicas de anonimização, **é importante que a Autoridade esclareça que (i) não é**

exigível bases legais suplementares para o processo de anonimização em si, de modo que o Estudo se alinhe com a experiência internacional, e (ii) uma vez implementada a técnica de anonimização, a LGPD deixa de ser aplicada não havendo de se verificar as finalidades conferidas às atividades de tratamento desses dados anonimizados.

b) Os riscos envolvidos na anonimização não podem ser sempre reduzidos a grandezas numéricas

Ao estabelecer uma abordagem baseada em risco, o Estudo Preliminar propõe a **quantificação do risco aceitável** e, em seguida, do **risco mensurado** como forma de avaliar de maneira matemática/estatística se o risco mensurado supera o risco aceitável (seção 3.2.2).

Embora a proposta se preste a indicar a necessidade de um juízo de proporcionalidade entre os riscos aceitável e o mensurado, **a redução destes elementos a grandezas numéricas não se mostra adequada por três motivos principais**: primeiro, o **risco aceitável**, como uma medida essencialmente valorativa e não matemática, não é capaz de oferecer a exatidão necessária para que a definição de um dado valor numérico seja mais do que o exercício de um mero arbítrio; segundo, o **risco mensurado,** como uma medida dos riscos efetivos, oferece dificuldades para ser reduzido a um número exato, já que **as ameaças conhecidas não são facilmente quantificáveis,** uma vez que dependem de contingências que trazem complexidade ao processo de aferição do risco; finalmente, algumas técnicas de anonimização (por exemplo, medidas não técnicas, de que são exemplos regramentos de governança) simplesmente não permitem a exata estimação numérica do riscos de reidentificação, sendo adequado para estas a possibilidade da avaliação qualitativa.[2]

Não por acaso, a Norma Brasileira da ABNT relativa a ISO 31000, sobre gestão de riscos, define probabilidade muito além das grandezas numéricas:

> *Na terminologia de gestão de riscos, a palavra probabilidade é utilizada para referir-se à chance de algo acontecer,* ***não importando se definida,***

[2] Uma amostra da complexidade que envolve a quantificação de riscos de reidentificação pode ser conferida no seguinte artigo, que recentemente propôs uma maneira nada trivial de realizá-la: Alvim M, Fernandes N, McIver A and Nunes G. A Quantitative Information Flow Analysis of the Topics API. Proceedings of the 22nd Workshop on Privacy in the Electronic Society. 2023. (123-127). Disponível em: https://dl.acm.org/doi/abs/10.1145/3589294

medida ou determinada, ainda que objetiva ou subjetivamente, qualitativa ou quantitativamente, e se descrita utilizando-se termos gerais ou matemáticos.[3] *(grifos nossos)*

Por isso, **a solução mais adequada,** capaz de abarcar todos os casos sem impor dificuldades técnicas e escolhas matemáticas arbitrárias aos agentes de tratamento, **seria a substituição das etapas do processo de anonimização pelo seguinte:**

1) aplicação das técnicas de anonimização, mantendo o que hoje se entende como "segunda etapa", mas com o esclarecimento de que a anonimização não se dá apenas por meios técnicos, devendo também abranger quaisquer outros processos empregados pelos agentes de tratamento que diminuam substancialmente o risco da identificação dos dados pessoais. Isso é, de certa forma dito pela ANPD no item 63 do Estudo Preliminar, contudo, no item 67, quando fala propriamente sobre a "segunda etapa", a ANPD traz uma abordagem mais restritiva, se referindo apenas aos "meios técnicos" utilizados;

2) avaliação, no caso concreto, se o risco de reidentificação é suficientemente baixo. Para este exame, como constante no guia da ICO (Autoridade de Proteção de Dados Britânica),[4] devem ser levados em conta o meios de uso provável para a reidentificação no caso concreto, considerando aspectos gerais do tratamento (como a finalidade), medidas de segurança aplicadas, custos e tempos envolvidos, competência necessária, possível motivação e tecnologias disponíveis;

3) asseguração da robustez da anonimização, o que caberia ser sugerido, pela ANPD, como boa prática e com a devida ressalva de serem considerados os meios técnicos razoáveis e disponíveis no momento em que o dado anonimizado estiver sendo tratado para se evitar insegurança jurídica e eventual ilegalidade retroativa, inadmissível pelo ordenamento jurídico.

[3] ABNT. Gestão de riscos - Diretrizes. Norma Brasileira. ABNT NBR ISO 31000. 2018, p.2.
[4] Cf. ICO. How do we ensure anonymisation is effective? Disponível em: https://ico.org.uk/media/about-the-ico/documents/4018606/chapter-2-anonymisation-draft.pdf

Assim, haveria maior espaço para a caracterização do que o Estudo Preliminar chama de Métrica Contextual, razão pela qual **a ANPD poderia expressamente reconhecer que não só que riscos quantificáveis sejam reduzidos a grandezas numéricas (como no caso da k-anonimização), mas também que cenários com riscos mais complexos (por exemplo, criptografia de padrões elevados) possam ser ponderados sem a necessidade de uma equação.**

c) Medidas organizacionais e regras de governança podem contribuir para a anonimização

Como bem notado na seção 3.1.3 do Estudo Preliminar, para a compreensão do processo de anonimização, em consonância com o que preceitua o art. 12 da LGPD, requer-se que sejam avaliados dois critérios: "esforços razoáveis" e "meios próprios", conceito ao qual a ANPD emprestou maior concretude em sua análise.

Para definir o conceito de **"esforços razoáveis"**, no Estudo cita-se o § 1º do referido artigo, que postula que "[a] determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios." Como admitido pelo Estudo, os elementos oferecidos pela LGPD (notadamente, custo, tempo e meios próprios) constituem um rol exemplificativo, havendo outros fatores objetivos que podem influir na caracterização de um dado como anônimo ou anonimizado.

Dentre estes fatores não mencionados mas admitidos pela Lei, destacam-se regramentos de governança de dados e outras medidas organizacionais dentro ou fora da estrutura dos agentes de tratamento, que podem desempenhar papel importante quando se trata de garantir a anonimização. Segundo o ICO, a Autoridade de Dados Britânica,

> *[i]f you anonymise personal data, your governance approach needs to address the practical issues surrounding the production and any disclosure of this information. Establishing an appropriate governance structure can improve your data management, record-keeping and disclosures of data. In addition, it is useful if you need to demonstrate compliance to the ICO.*

Afinal, é possível que agentes imponham, por fluxos de trabalho ou organização empresarial, o distanciamento dos elementos de reidentificação com relação ao contexto de tratamento dos dados anonimizados, fazendo com que os esforços necessários para eventual reidentificação sejam proibitivos em termos de custo e tempo, efetivamente caracterizando o dado como anonimizado a partir de fatores objetivos que o circundam.

Ademais, é importante ressaltar o precedente da *EU General Court*[5] quando da análise de caso no qual se discutia sobre anonimização/pseudonimização de dados e os esforços necessários e razoáveis para reidentificação. Segundo a Corte, que reforçou precedente da Corte de Justiça da União Europeia, em eventual compartilhamento de dados anonimizados por um agente de tratamento, **é preciso se colocar na posição do agente destinatário desse compartilhamento** para verificar se ele disporia dos códigos/meios necessários para realizar a reidentificação e/ou quais os esforços seriam demandados para tanto. Logo, a análise da possibilidade de reidentificação de dados e da qualidade de dados efetivamente anonimizados (ou não) deve ser feita considerando um agente específico de tratamento e não todo e qualquer agente de tratamento, nos mais diversos contextos.

O Estudo Preliminar deveria, portanto, explicitar que, para determinar se os dados são pseudonimizados ou anonimizados, é necessário considerar a perspectiva do destinatário dos dados, no momento da análise: se o destinatário não dispuser de quaisquer informações adicionais que lhe permitam reidentificar os titulares dos dados e não tiver, o destinatário, meios técnicos próprios disponíveis para obter tais informações, **os dados transmitidos devem ser considerados anonimizados e, portanto, não dados pessoais**.

Neste sentido, **eventual posicionamento da ANPD esclarecendo a relevância de medidas organizacionais para a garantia de anonimização se mostraria importante para a promoção de boas práticas de governança de dados, inclusive favorecendo a aplicação do art. 50 da LGPD.**

d) O caráter contínuo e iterativo da análise de anonimização deve ser esclarecido

5

O Estudo Preliminar define a anonimização como um processo contínuo (parágrafo 85). Nesse sentido, estabelece que a análise de robustez do processo de anonimização deve se dar repetidas vezes ao longo do tempo: "*[t]al avaliação não pode ser episódica ou pontual, mas sim iterativa e contínua, visto que novos riscos podem advir ao longo do tempo na medida dos avanços tecnológicos e da quantidade de dados auxiliares disponíveis, por exemplo*" (parágrafo 43).

É certo que avanços tecnológicos podem alterar as possibilidades de reidentificação de um determinado dado anônimo ou anonimizado, mas o estabelecimento de que a análise da robustez do processo de anonimização deve ser "iterativa e contínua" se beneficiaria de maior concretude quanto ao significado destas análises, sem que se implique em ônus excessivo para os agentes de tratamento. Isto é, **seriam mais que bem-vindos esclarecimentos exemplificativos da ANPD a respeito da conformação da análise iterativa, respondendo se se refere à repetição total ou simplificada da análise inicial, ou se se refere à higienização da base de dados, sendo esta última hipótese certamente a preferível.**

Ao disponibilizar recomendações relativas à análise "iterativa e contínua", a ANPD não só garantiria mais segurança jurídica aos agentes de tratamento, mas também estabeleceria de modo público os seus próprios critérios sugestivos para configuração de um bom acompanhamento ao longo do tempo da anonimização.

5. A ANPD deve incentivar a adoção de tecnologias avançadas de anonimização

As chamadas *privacy-enhancing technologies* (PETs) são, conforme definição da ENISA (Agência Europeia de Cibersegurança), "*software and hardware solutions, i.e. systems encompassing technical processes, methods, or knowledge to achieve specific privacy or data protection functionality or to protect against risks to privacy of an individual or a group of natural persons*."

Nesta condição, incluem-se entre as PETs tecnologias avançadas de anonimização, como a criptografia homomórfica e dados sintéticos, capazes de diminuir substancialmente o risco de reidentificação dos titulares de dados pessoas.

Entretanto, considerando que as PETs apresentam alta complexidade e implicam custos de desenvolvimento, os agentes podem necessitar de incentivos para implementá-las. **Um grande estímulo seria a ANPD reconhecer a eficácia da à aplicação de PETs**

para fins de anonimização, o que daria segurança jurídica para sua custosa implementação e assim se afiguraria como um incentivo ao aperfeiçoamento técnico da proteção da privacidade.

A este propósito, pode haver também o incentivo à manutenção de registros e documentação para o processo de anonimização, compreendendo as avaliações de risco e informações sobre técnicas utilizadas – sem ignorar preocupações com segurança, já que a publicização indevida desta documentação tende a aumentar os riscos de reidentificação. A este propósito, pronuncia-se a Autoridade de Dados de Cingapura:

> *"As good practice, the details of the anonymisation process, parameters used and controls should also be clearly recorded for future reference. Such documentation facilitates review, maintenance, fine-tuning and audits.* ***Note that such documentation should be kept securely as the release of the parameters may facilitate re-identification and disclosure of the anonymised data****."*[6]

Desta forma, a ANPD passaria a ter meios concretos para aferir a aderência às boas práticas de anonimização ao mesmo tempo em que garantiria segurança jurídica aos agentes de tratamento para a implementação de tecnologias avançadas de proteção à privacidade.

6. Alocação de responsabilidades pelas próprias partes

Embora o Estudo Preliminar não o mencione claramente, no mercado é prática comum que agentes de tratamento **recebam dados já anonimizados por outro agente** que realizou previamente o processo de anonimização, elegendo, entre outros, os meios técnicos utilizados.

Dada a pluralidade de relações que podem existir do uso e compartilhamento de dados anonimizados, em consonância com a autonomia da vontade e liberdade contratual das

[6] "*Como boa prática, os detalhes do processo de anonimização, os parâmetros utilizados e os controlos também devem ser claramente registrados para referência futura. Essa documentação facilita a revisão, manutenção, ajuste fino e auditorias. Note-se que essa documentação deve ser mantida em segurança, uma vez que a divulgação dos parâmetros pode facilitar a reidentificação e divulgação dos dados anonimizados*." (tradução livre) V. PDPC, p. 26

partes[7], **seria interessante que o Estudo deixasse aos agentes de tratamento a questão referente à alocação de responsabilidades - sobretudo quanto ao acompanhamento dos riscos da reidentificação - uma vez que mais próximos e com uma melhor compreensão da(s) relação(ões) jurídica(s) na(s) qual(ais) estão envolvidos, evitando, assim, qualquer predeterminação pela ANPD.** Isso porque as regras de responsabilidade já estão definidas em lei e cabem aos agentes de tratamento, conforme as tratativas realizadas e obrigações assumidas nas relações negociais nas quais envolvidos, responder por eventual ilicitude ou inadimplemento conforme legalmente delineado, ou contratualmente estabelecido.

9. Das alternativas conferidas pela LGPD à eliminação dos dados pessoais

O Estudo Preliminar da ANPD adotou o posicionamento no sentido de que, quando houver eventual desconformidade no tratamento de dados pessoais, a eliminação dos dados pessoais tratados seria a solução a ser adotada pelo controlador.

Esse posicionamento, contudo, restringe as possibilidades existentes ao controlador de dados, conclusão que se chega não só por interpretação da própria LGPD, como também pela abordagem decorrente de uma regulação responsiva que a ANPD defende e adota. Isso porque, há outras formas de trazer o tratamento de dados à conformidade que não seja necessária e exclusivamente a eliminação dos dados, a exemplo do artigo 18 IV da LGPD, no qual traz o bloqueio de dados pessoais ou a anonimização como alternativas, como também pelo artigo 52 da LGPD, que traz a advertência, ou o bloqueio de dados como sanções viáveis.

Deste modo, e tendo em vista que a presente contribuição se refere ao tema de anonimização dos dados, é importante que a ANPD esclareça a possibilidade de sua adoção como medida de trazer o tratamento de dados pessoais à eliminação.

10. As consequências jurídicas da reidentificação de dados antes anonimizados

[7] CC/02: Art. 421. A liberdade contratual será exercida nos limites da função social do contrato. Parágrafo único. Nas relações contratuais privadas, prevalecerão o princípio da intervenção mínima e a excepcionalidade da revisão contratual

Ao longo do Estudo, acertadamente fala-se sobre riscos de reidentificação como aspecto essencial para uma abordagem da anonimização baseada em riscos. Ainda assim, não há referências às consequências jurídicas que adviriam da efetiva reidentificação de um determinado dado ou conjunto de dados pessoais anonimizados.

Neste sentido, seria salutar que a ANPD, em reforço ao seu papel educativo e em consonância com seu entendimento de que a **anonimização não pressupõe total irreversibilidade**, auxiliasse e melhor instruísse, os agentes de tratamento, ao, por exemplo, (i) divulgar quando uma nova tecnologia for identificada; (ii) emitir diretrizes sobre maneiras de recondução à conformidade caso; (iii) elaborar recomendações sobre técnicas reconhecidamente eficientes relacionadas à anonimização, sendo sempre fundamental a ênfase na observância das medidas técnicas razoáveis e disponíveis pelos agentes no momento do tratamento.

11. Etapas da pseudonimização devem ter clara natureza de recomendação

No Estudo Preliminar (p. 22), afirma-se ser fundamental a adoção de uma metodologia eficaz de pseudonimização. Em sequência, a Autoridade menciona que a metodologia eficaz **deve** considerar doze etapas, incluindo o desenvolvimento de políticas, de treinamentos, auditoria, RIPD, entre outros aspectos.

Considerando a linguagem empregada, é possível que essas etapas sejam consideradas para fins de fiscalização, gerando mais encargos aos agentes de tratamento que desejam se adequar à legislação, sem, contudo, contar com correspondentes na legislação ou na regulamentação da Lei pela ANPD.

Neste contexto, **seria salutar que a Autoridade esclarecesse que as etapas da pseudonimização constituem uma recomendação relativa ao tema, e não são deveres em si mesmos.**

12. Processo de anonimização e intervenção humana

No Apêndice do Estudo Preliminar, alínea k, afirma-se que a "anonimização não **deve** ser totalmente automatizada", e em seguida se assume que "dada a importância do contexto e a avaliação geral do processo, **poderá** ser necessária a intervenção de um especialista humano". A construção apresentada nesta alínea nos parece contraditória porquanto não fica claro se a ANPD quis determinar a necessidade de intervenção

humana no processo de anonimização ou se pretendeu deixar a critério do agente de tratamento essa decisão.

Como a LGPD não exige obrigatoriamente tal intervenção, mas ao contrário, permite, para tanto a utilização de quaisquer "meios técnicos razoáveis e disponíveis na ocasião de seu tratamento" (art. 5º, III), a intervenção humana, por consequência, é uma possibilidade a ser implementada se assim os agentes de tratamento entenderem cabível e segundo sua própria avaliação de risco. Logo, não pode ser tratada como um requisito necessário do processo de anonimização, **pelo que se sugere à ANPD a retificação da redação da alínea k para seja mais clara nesse sentido, qual seja, no processo de a anonimização a intervenção humana é facultativa e cabe ao agente de tratamento decidir sobre sua conveniência.**

Contribuição CIR Samsung
"Consulta à Sociedade – Estudo Preliminar – Anonimização e pseudonimização para proteção de dados"

Parágrafo nº 27

A partir da análise do art. 12, caput, da LGPD, compreende-se que a utilização de meios técnicos na anonimização de dados consiste, na verdade, em um conjunto de atos ou medidas entre si relacionadas que fazem parte de um processo. Dessa forma, a anonimização se desenvolve em uma série de etapas que se inicia com o processamento de dados pessoais e tem o objetivo de, com a aplicação de técnicas variadas, desassociar identificadores do dado em seu estado originário ou bruto.

Contribuição CIR Samsung

A ênfase da ANPD no processo de anonimização em várias etapas, conforme articulado no Artigo 12 da LGPD, destaca a necessidade de **diretrizes claras para os controladores de dados pessoais que recebem dados previamente anonimizados**. Embora a anonimização represente uma etapa crítica na proteção de dados pessoais, é imperativo garantir que os controladores de dados pessoais que recebem tais dados estejam em conformidade com os padrões da LGPD e da ANPD para manter a integridade e proteção dos dados pessoais.

Nesse sentido, salvaguardas claras devem ser estabelecidas para orientar os controladores no tratamento de dados pessoais previamente anonimizados de forma eficaz. Fornecer orientação abrangente a esse respeito não apenas aumenta a certeza jurídica, mas também promove a consistência nas práticas de proteção de dados pessoais e fortalece a confiança entre os controladores de dados pessoais e os titulares, alinhando-se aos princípios fundamentais da LGPD.

Diante do exposto, proponho que a ANPD considere as seguintes medidas para abordar o tratamento de dados pessoais previamente anonimizados:

1. **Verificação de Técnicas de Anonimização**: Os controladores de dados pessoais devem realizar avaliações minuciosas para verificar se as técnicas de anonimização utilizadas pelo controlador anterior estão em conformidade com os padrões da LGPD, dissociando efetivamente os identificadores dos dados pessoais originais. Isso garante que os dados pessoais anonimizados mantenham sua integridade e proteção.
2. **Medidas de Diligência**: Os controladores de dados pessoais devem realizar medidas de diligência para validar a legitimidade das atividades de processamento originais e garantir alinhamento com os propósitos e bases legais da LGPD. Isso envolve avaliar a legalidade e adequação das atividades de processamento inicial que levaram à anonimização.
3. **Transparência e Responsabilidade**: Deve ser enfatizada a transparência e responsabilidade no tratamento de dados previamente anonimizados. Os controladores de dados pessoais devem manter registros documentando a origem e natureza dos dados recebidos e quaisquer avaliações realizadas para validar sua conformidade com os requisitos da LGPD. Isso promove transparência e responsabilidade nas atividades de processamento de dados.

Ao implementar essas medidas, os controladores de dados pessoais podem navegar eficazmente pelas complexidades do tratamento de dados previamente anonimizados

enquanto cumprem os padrões da LGPD. Além disso, fornecer orientações claras sobre esse assunto contribuirá para a eficácia geral das práticas de proteção de dados no Brasil e fomentará a confiança no ecossistema digital.

Em conclusão, insto a ANPD a incorporar essas sugestões nas diretrizes sobre Anonimização e Pseudonimização para garantir uma proteção robusta dos dados pessoais e facilitar o cumprimento dos padrões da LGPD.

Parágrafo nº 27

A partir da análise do art. 12, caput, da LGPD, compreende-se que a utilização de meios técnicos na anonimização de dados consiste, na verdade, em um conjunto de atos ou medidas entre si relacionadas que fazem parte de um processo. Dessa forma, a anonimização se desenvolve em uma série de etapas que se inicia com o processamento de dados pessoais e tem o objetivo de, com a aplicação de técnicas variadas, desassociar identificadores do dado em seu estado originário ou bruto.

Contribuição CIR Samsung

Esta ilustre Autoridade tem promovido fóruns em diversas ocasiões para discutir o potencial dos dados pessoais anonimizados utilizados no treinamento de inteligência artificial (IA) em gerar dados sintéticos que poderiam ser classificados como dados pessoais. Essa perspectiva representa uma alteração significativa de paradigma na concepção de dados pessoais, destacando a complexidade da anonimização de dados e da proteção da privacidade. Dado que os algoritmos de IA têm capacidades preditivas que podem inferir informações pessoais a partir de conjuntos de dados aparentemente anonimizados, torna-se urgente realizar uma análise minuciosa e estabelecer diretrizes claras sobre este assunto.

Ante este cenário, **é crucial que a ANPD explore como os dados pessoais anonimizados, quando utilizados no treinamento de IA, podem potencialmente ser revertidos ou transformados em dados pessoais**. Isso demanda uma compreensão sutil dos mecanismos pelos quais os algoritmos de IA extrapolam e inferem informações, mesmo a partir de fontes aparentemente anonimizadas.

Nesse contexto, a Samsung considera fundamental que a ANPD forneça diretrizes claras para **definir dados sintéticos derivados de fontes anonimizadas sob a LGPD**. Isso inclui especificar o limiar no qual os dados sintéticos indicam características ou comportamentos individuais suficientemente para justificar a classificação como dados pessoais. Essa clareza auxiliará os controladores de dados e os usuários de IA a navegarem pelas complexidades das regulamentações de proteção de dados, ao mesmo tempo que promove práticas de desenvolvimento de IA responsáveis que priorizam os direitos de privacidade dos indivíduos.

Apesar de compreender a complexidade desse quadro, a Samsung acredita que abordar as implicações dos dados anonimizados no treinamento de IA sob a LGPD é crucial para garantir padrões robustos de proteção de dados no Brasil. Reconhecemos que este assunto pode exigir uma análise e consideração adicionais por parte da ANPD que não cabem a este guia. Portanto, estamos abertos à possibilidade de apresentar nossas contribuições à Autoridade em oportunidades futuras ou quando esta se manifestar sobre o assunto.

Parágrafo nº 47

A compreensão do processo de anonimização e dos critérios a serem considerados para avaliar os riscos de reidentificação, requer, necessariamente, a interpretação de dois termos previstos no artigo 12 da LGPD: “esforços razoáveis” e “meios próprios”.

Contribuição CIR Samsung

O reconhecimento da ANPD da necessidade de interpretar "esforços razoáveis" no contexto das atividades de anonimização destaca a complexidade de garantir a proteção de dados ao mesmo tempo em que facilita operações legítimas de tratamento de dados. No entanto, a vagueza desses termos apresenta desafios para os agentes de tratamento de dados pessoais na compreensão e implementação de medidas adequadas de anonimização.

Para facilitar a conformidade com a LGPD e promover práticas eficazes de anonimização, a Samsung recomenda que a ANPD forneça critérios claros e objetivos para "esforços razoáveis".

Além disso, a ANPD poderia **compilar e atualizar regularmente uma lista de atividades adequadas de anonimização**, oferecendo orientações práticas aos tratamento de dados pessoais. Isso ajudaria a garantir o alinhamento com os requisitos da LGPD e promoveria consistência nas práticas de anonimização em diferentes organizações.

Dada a natureza em constante evolução da tecnologia, especialmente com o aumento do uso de inteligência artificial (IA), a definição de "esforços razoáveis" se apresenta um conceito cada vez mais fluido. Portanto, a ANPD deve se comprometer a revisar regularmente os critérios objetivos usados para determinar esta questão. Disponibilizar publicamente os processos administrativos relacionados a este tópico permitiria que os agentes de tratamento de dados adaptassem seus processos internos de acordo com a interpretação em evolução da ANPD.

Em conclusão, ao fornecer clareza e objetividade na avaliação de esforços razoáveis para anonimização sob a LGPD, a ANPD pode facilitar a conformidade com as regulamentações de proteção de dados e promover práticas eficazes de anonimização de dados que protejam os direitos de privacidade dos indivíduos.

Parágrafo nº 82

É importante observar que a LGPD enfatiza que, para que a pseudonimização seja eficaz, as informações adicionais que permitem a reversão da pseudonimização (por exemplo, as chaves criptográficas) devem ser mantidas separadamente e protegidas por medidas técnicas e organizacionais adequadas. Além disso, a LGPD enfatiza a importância de garantir a privacidade e a segurança dos dados pessoais em todas as etapas do tratamento. Portanto, a escolha da técnica de pseudonimização deve ser feita com cuidado, levando em consideração o contexto, os riscos associados e a sensibilidade dos dados.

Contribuição CIR Samsung

Em relação ao estudo preliminar da Autoridade Nacional de Proteção de Dados (ANPD) sobre práticas de anonimização e pseudonimização, é essencial enfatizar a preocupação com a reversibilidade da pseudonimização e ressaltar a importância fundamental dos processos de criptografia para garantir sua irreversibilidade.

A Lei Geral de Proteção de Dados (LGPD) destaca que, para que a pseudonimização seja verdadeiramente eficaz, as informações adicionais necessárias para reverter o processo, como as chaves criptográficas, devem ser gerenciadas separadamente e protegidas por medidas técnicas e organizacionais apropriadas. Esta separação e proteção são essenciais para assegurar que os dados permaneçam seguros e protegidos contra acessos não autorizados ou uso indevido.

Além disso, a LGPD enfatiza a importância de garantir a privacidade e a segurança dos dados pessoais em todas as fases do tratamento. Portanto, ao escolher a técnica de pseudonimização a ser empregada, é crucial considerar cuidadosamente o contexto específico, os riscos associados e a sensibilidade dos dados envolvidos.

É imperativo que os responsáveis pelo tratamento de dados adotem medidas robustas de segurança, não apenas para proteger os dados em si, mas também para salvaguardar as chaves criptográficas e os algoritmos utilizados no processo de pseudonimização. Essas medidas são essenciais para prevenir acessos não autorizados, garantir a integridade dos dados e assegurar que a pseudonimização seja irreversível, conforme preconizado pelos princípios da LGPD.

Portanto, recomenda-se que a ANPD adote uma abordagem rigorosa na definição de diretrizes e regulamentações relacionadas à pseudonimização, incentivando a implementação de práticas de criptografia robustas e a conscientização sobre a importância de proteger as chaves criptográficas como parte integral do processo de pseudonimização, assim como incentive agentes de tratamento que implementem estas técnicas por meio da avaliação como boa governança pelo uso destas técnicas.

Sendo assim, sugere-se o seguinte texto para este parágrafo:

É importante observar que a LGPD enfatiza que, para que a pseudonimização seja eficaz, as informações adicionais que permitem a reversão da pseudonimização (por exemplo, as chaves criptográficas) devem ser mantidas separadamente e protegidas por medidas técnicas e organizacionais adequadas. **A utilização de técnicas eficazes para garantir que essas chaves criptográficas não estejam acessíveis será considerada uma boa prática, podendo acarretar eventual afastamento de responsabilização em eventos adversos**. Além disso, a LGPD enfatiza a importância de garantir a privacidade e a segurança dos dados pessoais em todas as etapas do tratamento. Portanto, a escolha da técnica de pseudonimização deve ser feita

com cuidado, levando em consideração o contexto, os riscos associados e a sensibilidade dos dados.

Paulo Henrique Atta Sarmento
OAB/DF nº 63.259
OAB/SP nº 457.362

Leonardo Werlang
OAB/PR nº 47.985

Juliana Pereira Cortes
OAB/SP nº 375.700

LAPIN
LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET

Considerações do LAPIN à Consulta sobre o Estudo Preliminar de Anonimização e Pseudonimização da ANPD

O Laboratório de Políticas Públicas e Internet (LAPIN) é um centro de pesquisa e ação independente de composição multidisciplinar com sede na capital federal brasileira. Seu objetivo é apoiar o desenvolvimento de políticas públicas voltadas para a regulação das tecnologias digitais por meio da pesquisa e da conscientização da sociedade.

Faz parte das missões do LAPIN a contribuição ao processo regulatório da proteção de dados e a construção de uma cultura de proteção de dados pessoais.

A partir da leitura do estudo preliminar e os estudos técnicos realizados pela Autoridade Nacional de Proteção de Dados (ANPD) lançados no âmbito da consulta sobre anonimização e pseudonimização para proteção de dados aberta no dia 30 de janeiro de 2024, o LAPIN entende como o importante o panorama sobre o tema dado pela autoridade.

A fim de dar prosseguimento ao debate e de contribuir com o trabalho de regulação e orientação da ANPD, o LAPIN realiza as seguintes contribuições:

1. Para os que produzem e fiscalizam as normas, diversos desafios tornam o caminho mais denso, como pensar em um equilíbrio entre a sociedade e os agentes econômicos, em como manter a inovação sem ferir os direitos individuais. Em que pese a ANPD tenha avançado no tema com importantes considerações e termos base que serão utilizados no futuro da regulação, assim como com a apresentação de exemplos de técnicas usadas no campo, ainda são necessários esforços para a difusão da anonimização e pseudonimização no ecossistema de proteção de dados.

2. Considera-se que a anonimização é um tema que exige constante atualização técnica para a avaliação da razoabilidade e disponibilidade dos meios técnicos empregados com a finalidade de anonimização. O LAPIN, assim, considera importante que a ANPD estabeleça uma **agenda de atualização periódica** sobre o **estado da arte** da anonimização, de forma que o corpo técnico da autoridade possua meios institucionais para a pesquisa e a capacitação sobre as técnicas razoáveis e disponíveis de anonimização. Neste sentido, de início, é possível imaginar medidas como **programas de capacitação**, **linhas internas de pesquisa**, **instrumentos de colaboração com academia, setor privado e terceiro setor**. Tal medida terá importante papel na atuação fiscalizatória e sancionatória do órgão, bem como poderá servir de base para o planejamento de atualização dos próprios agentes de tratamento.

3. Recomenda-se que a ANPD deverá estruturar a sua atuação em termos **fiscalizatórios e sancionatórios** diante dos agentes de tratamento que realizam processos de anonimização e dos titulares de dados que recorrem ao órgão para a efetivação deste direito. Assim, recomenda-se que a ANPD estabeleça **diretrizes específicas** elencando **prioridades**, **critérios mínimos** de avaliação na fiscalização e a criação de uma **metodologia** e procedimentos padrão para este fim.

4. Em que pese a anonimização de dados pessoais não estar limitada à esfera de **direitos dos titulares**, é fato que a LGPD prevê em seu artigo 18, inciso IV que o titular de dados tem o direito de requerer ao controlador, a qualquer momento, a anonimização de dados pessoais desnecessários, excessivos ou tratados em desconformidade com a lei. Desta forma, a ANPD deve estruturar orientações para os agentes de tratamento no que diz respeito à **operacionalização de tais solicitações**, desde a avaliação de sua possibilidade, realização, documentação e comunicação ao titular. Por outro lado, os titulares de dados também devem receber **informações didáticas** sobre esse direito e as **condições de atendimento de eventual pedido**.

6. O LAPIN considera de grande importância a garantia de **participação da sociedade organizada nos processos administrativos** que envolvam anonimização e pseudonimização, assim como nos próximos passos da agenda regulatória. A ANPD deve garantir nessas atuações processos de **transparência ativa e passiva**.

7. Elaboração de **materiais de conscientização e educação** em proteção de dados. A participação e as demandas da sociedade são intrínsecas à construção de uma cultura que abarque o conhecimento necessário para que estes gozem de seus direitos e em certa medida façam com que os propósitos da lei sejam atingidos. O LAPIN recomenda que a ANPD elabore **cartilhas, vídeos educativos e até mesmo ações de conscientização no tema**.

8. Seguindo esta linha de raciocínio, o LAPIN reconhece a necessidade de ampliar os esforços de conscientização e educação em proteção de dados, especialmente para os **agentes de tratamento de pequeno porte**. Nesse sentido, é fundamental que sejam elaborados **manuais** específicos que abordem técnicas de anonimização e pseudonimização adaptadas às particularidades desses agentes, seguindo o modelo estabelecido pelo Guia de Segurança da Informação para Agentes de Tratamento de Pequeno Porte, publicado em 04 de outubro de 2021. Esses materiais devem fornecer orientações práticas e acessíveis, facilitando a implementação das melhores práticas de proteção de dados nesse segmento crítico, promovendo assim um ecossistema de dados mais seguro e alinhado com os princípios da Lei Geral de Proteção de Dados (LGPD). Esta iniciativa não só aumentará a conformidade regulatória entre os pequenos agentes, mas também fortalecerá a proteção dos direitos dos titulares de dados em todo o país.

9. Além do guia mencionado, é imprescindível que seja fornecido um **manual de ferramentas e técnicas** de anonimização especificamente destinado às Pequenas e Médias Empresas (PMEs), detalhando de forma exemplificativa, ainda que não exaustiva, os tipos de dados nos quais essas técnicas podem ser aplicadas. Esse manual servirá como uma ferramenta prática para orientar as PMEs na identificação rápida e eficiente dos dados sensíveis ou pessoais que requerem tratamento através da anonimização ou pseudonimização, garantindo assim maior proteção e conformidade com a LGPD.

REALIZAÇÃO

Laboratório de Políticas Públicas e Internet - LAPIN

AUTORIA

Luiza Xavier Morales

Tayrone Marquesini Chiavone

REVISÃO

Cynthia Picolo Gonzaga de Azevedo

São Paulo, 14 de março de 2024.

À
AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)
normatizacao@anpd.gov.br

Ref.: Estudo Preliminar – Anonimização e Pseudonimização para a proteção de dados pessoais

Prezados,

A **Associação Brasileira de Instituições de Pagamentos** ("**ABIPAG**"), inscrita no CNPJ/ME sob o nº26.425.404/0001-10, vem respeitosamente à presença desta Autoridade Nacional de Proteção de Dados ("**ANPD**") apresentar contribuições à consulta acerca do estudo preliminar sobre anonimização e pseudonimização para a proteção de dados pessoais.

A ABIPAG é uma associação setorial do mercado de meios de pagamentos eletrônicos formada por instituições de pagamento e instituições financeiras. Nesse sentido, suas contribuições possuem como foco o melhor interesse do titular de dados e estão direcionadas à realidade do mercado de meios de pagamento.

SUMÁRIO EXECUTIVO

A ABIPAG envia, em anexo, tabela contendo sugestões de alteração do texto proposto com o intuito de garantir práticas mais benéficas para usuários, agentes de tratamento e encarregados. Dentre os principais pontos, encontram-se propostas para:

Uniformizar definições: Para evitar interpretações divergentes e garantir segurança jurídica aos agentes regulados, a ABIPAG sugere que haja uma padronização do significado dos termos do Glossário deste Guia com base no Glossário de Proteção de Dados Pessoais e Privacidade elaborado pela ANPD[1]. A ABIPAG também reforça a necessidade de que o documento utilizado como base tenha revisão periódica com a finalidade de garantir a atualização devida;

Não responsabilizar pela Reidentificação: Com fundamento no art. 5º, XI, da Lei Geral de Proteção de Dados[2], a anonimização é uma medida que objetiva a impossibilidade de associação, direta ou indireta, de um dado e/ou conjunto de

[1] https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/glossario-anpd-protecao-de-dados-pessoais-e-privacidade.pdf
[2] Lei nº 13.709/2018

dados a um indivíduo. A técnica adotada para o processo de anonimização deve ser considerada irreversível somente até a extensão das técnicas atuais. Nesse sentido, a ABIPAG tece sugestão no texto para reforçar que, caso seja criada técnica no futuro capaz de reverter o processo de anonimização, os agentes sujeitos à regulação não devem ser responsabilizados por tratamentos pretéritos (desde que tenham realizado tudo o que era necessário dentro dos instrumentos técnicos que possuíam à época);

Atribuir natureza de recomendação à sugestão das etapas de pseudonimização: Com a finalidade de evitar interpretação que sugira obrigatoriedade à implementação dos fluxos indicados no Guia, a ABIPAG sugere alteração na redação que esclareça o caráter exemplificativo das etapas abordadas. .

Possibilitar a automatização completa da anonimização: A automatização total do processo de anonimização poderia reduzir erros humanos e garantir a aplicação das mesmas regras de forma consistente, aprimorando a segurança do fluxo como um todo, sendo o único desafio a comprovação de eficácia do processo. Por essa razão, a ABIPAG sugere que adequação de redação para permitir a automatização total da anonimização, condicionada à revisão periódica da eficácia do processo por um especialista humano.

Para uma compreensão mais específica dessas propostas, a ABIPAG encaminha a tabela anexa, em que cada ponto será abordado em detalhe.

***

Sendo o que servia para o momento, a ABIPAG se coloca à inteira disposição da ANPD para prestar esclarecimentos adicionais que se façam necessários.

Atenciosamente,

ABIPAG – ASSOCIAÇÃO BRASILEIRA DE INSTITUIÇÕES DE PAGAMENTOS

Parágrafo do Guia	Sugestão da ABIPAG	Justificativa
2.1 GLOSSÁRIO Banco de dados: Conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico. Conjunto de dados: Vide Banco de dados.	2.1 GLOSSÁRIO Banco de dados: Conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico. Conjunto de dados: conjunto estruturado de dados organizados e armazenados de forma a possibilitar o seu acesso, recuperação, modificação e gestão eficientes.	Considerando a utilização do termo "dados pessoais" na definição de Banco de Dados no Glossário, a ABIPAG sugere que haja diferenciação para o conceito de Conjunto de dados, permitindo que este não necessariamente envolva apenas dados pessoais.

Parágrafo do Guia	Sugestão da ABIPAG	Justificativa
-	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.	Sugere-se que seja incluído o conceito de pseudonimização adotado pelo Glossário de Proteção de Dados Pessoais e Privacidade elaborado pela ANPD, facilitando a compreensão do documento. A ABIPAG também reforça a necessidade de que esse documento utilizado como base tenha revisão periódica com a finalidade de garantir a atualização devida.
14. O Identificador direto é o dado que por si só permite identificar unicamente uma pessoa natural, sem a necessidade de combiná-lo com dados de outras fontes. O típico identificador direto de um titular de dados é o seu nome completo. Outro exemplo é o número de inscrição no Cadastro de Pessoas Físicas (CPF), que é considerado número único e suficiente para identificação do cidadão nos bancos de dados de serviços públicos, nos termos da Lei nº 14.534/2023.	14. O Identificador direto é o dado que por si só permite identificar unicamente uma pessoa natural, sem a necessidade de combiná-lo com dados de outras fontes. O típico identificador direto de um titular de dados é ~~o seu nome completo. Outro exemplo é~~ o número de inscrição no Cadastro de Pessoas Físicas (CPF), que é considerado número único e suficiente para identificação do cidadão nos bancos de dados de serviços públicos, nos termos da Lei nº 14.534/2023	Para evitar eventual identificação equivocada da pessoa física em razão da existência de homônimos, a ABIPAG recomenda a exclusão do exemplo do nome completo como identificador direto.
23. Os dados pessoais, quando submetidos a processos de anonimização e pseudonimização, passam por alterações que visam a impedir sua associação direta ou indireta a um indivíduo específico. A distinção crucial entre dados anonimizados e pseudonimizados reside na reversibilidade do processo e na capacidade reversibilidade do processo e na capacidade de restabelecer a associação com a identidade original do indivíduo.	23. Os dados pessoais, quando submetidos a processos de anonimização e pseudonimização, passam por alterações que visam a impedir sua associação direta ou indireta a um indivíduo específico. A distinção crucial entre dados anonimizados e pseudonimizados reside na reversibilidade do processo e na capacidade de restabelecer a associação com a identidade original do indivíduo, no momento do tratamento do dado	Recomenda-se a inclusão de marco temporal para evitar que as empresas que adotarem medidas de segurança e transparência utilizando os meios técnicos disponíveis no momento do tratamento de dados sejam responsabilizadas por eventual reidentificação realizada com base em tecnologia não disponível à época.

Parágrafo do Guia	Sugestão da ABIPAG	Justificativa
54. convém ressaltar que os dados que tenham sido tornados irreversivelmente anonimizados deixam de ser considerados "dados pessoais" e o processamento desses dados não exige conformidade com a legislação de proteção de dados. Isso implica que as organizações podem utilizá-los para finalidades, desde que compatíveis, que vão além daquelas para as quais foram originalmente coletados e esses dados podem ser mantidos indefinidamente.	54. convém ressaltar que os dados que tenham sido tornados irreversivelmente anonimizados deixam de ser considerados "dados pessoais" e o processamento desses dados não exige conformidade com a legislação de proteção de dados. Isso implica que as organizações podem utilizá-los para outras finalidades, desde que compatíveis com as que originaram a coleta do dado, bem como que esses dados podem ser mantidos indefinidamente.	A ABIPAG sugere alteração do texto para que conste expressamente qual o limite da utilização de dados após deixarem de ser considerados dados pessoais.
84.Conforme ilustração acima (Figura 3), para o desenvolvimento dessa metodologia algumas etapas devem ser observadas:	84.Conforme ilustração incluída acima (Figura 3) apenas para fins exemplificativos, para o desenvolvimento dessa metodologia algumas etapas podem ~~devem~~ ser observadas:	Para evitar interpretações subjetivas acerca da obrigatoriedade de fluxo nos termos da imagem, a ABIPAG sugere a inclusão de menção expressa ao caráter meramente exemplificativo da ilustração elencada no Guia.
k) A anonimização não deve ser totalmente automatizada - ferramentas automatizadas podem ser usadas durante o processo de anonimização, no entanto, dada a importância do contexto e a avaliação geral do processo, poderá ser necessária a intervenção de um especialista humano	k) ~~A anonimização não deve ser totalmente automatizada~~ Ferramentas automatizadas podem ser usadas durante o processo de anonimização, no entanto, dada a importância do contexto e a avaliação geral do processo, poderá ser necessária a intervenção de um especialista humano	A automatização total do processo de anonimização poderia reduzir erros humanos e garantir a aplicação das mesmas regras de forma consistente, aprimorando a segurança do fluxo como um todo, sendo o único desafio a comprovação de eficácia do processo. Por essa razão, a ABIPAG sugere que adequação de redação para permitir a automatização total da anonimização, condicionada à revisão periódica da eficácia do processo por um especialista humano.

contato@bbladv.com.br
www.bbladv.com.br

ESTUDO PRELIMINAR SOBRE ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO PARA PROTEÇÃO DE DADOS PESSOAIS

ASSUNTO: Contribuições sobre o Estudo Preliminar sobre anonimização e pseudonimização para proteção de dados pessoais submetido à consulta pela Autoridade Nacional de Proteção de Dados (ANPD).

I. Considerando o conteúdo do Estudo Preliminar, apresente suas contribuições sobre o texto.

Este documento tem como objetivo contribuir para o aprimoramento da regulamentação brasileira, oferecendo *insights* práticos e orientações internacionais sobre a matéria, a fim de auxiliar os agentes de tratamento na aplicação efetiva da anonimização e pseudonimização:

(a) Pseudonimização para a mitigação de risco em caso de incidente de segurança

Embora o Guia mencione a possibilidade de utilização de pseudonimização como parte de uma estratégia de "minimização de dados", o documento não confere a devida relevância à pseudonimização na mitigação de riscos em caso de incidente de segurança envolvendo dados pessoais. Além de contribuir para minimizar a exposição dos dados pessoais, a pseudonimização é de mais fácil implementação pelos agentes de tratamento e reduz drasticamente os impactos das violações de dados pessoais, sendo, portanto, uma alternativa eficaz.

O Guia também não esclarece se a implementação de técnicas de pseudonimização traz implicações nos deveres dos agentes de tratamento quando há ocorrência de incidente de segurança. A título de exemplo, o Regulamento Geral de Dados Europeu (RGPD), estabelece que no caso de incidentes de segurança que afetem dados pessoais ininteligíveis para terceiros em razão da aplicação de técnicas de pseudonimização, como a criptografia, não é necessário comunicar ocorrência do incidente aos titulares de dados, uma vez que as informações afetadas

estão protegidas por medidas de segurança que não permitiriam a identificação do titular (art. 33.3 "a", RGPD).

Conforme disposto na LGPD, a comunicação de incidente de segurança é necessária quando o evento acarretar risco ou dano relevante aos titulares de dados. Portanto, a dispensa à comunicação aos titulares quando os dados afetados por incidente sejam pseudonimizados estaria alinhada com os critérios da LGPD, já que ao tornar as informações ininteligíveis, não seria configurado risco ou dano relevante ao titular.

Sugerimos, assim, que esses pontos sejam abordados pela Autoridade no Estudo Técnico, a fim de elucidar o tema de pseudonimização aos agentes de tratamento, bem como acerca das implicações práticas decorrentes de sua implementação.

(b) Distinção entre operação de tratamento de dados e implementação de anonimização

Uma leitura superficial do texto do Estudo Técnico pode levar ao entendimento de que o processo de anonimização implica em uma nova operação de tratamento de dados. Isso se deve ao fato de o texto dispor que, ao implementar a técnica, os agentes de tratamento devem identificar a base legal para a coleta dos dados a serem anonimizados, informar os titulares dos dados do processo de anonimização e avaliar a compatibilidade da anonimização com os propósitos inicialmente definidos para o tratamento de dados.

No entanto, é importante esclarecer que o processo de anonimização não é caracterizado como uma operação de tratamento de dados pessoais. Pelo contrário, trata-se de um meio alternativo ao tratamento que visa proteger o titular de dados através da desidentificação da informação, sendo, assim, uma medida para conciliar os interesses das organizações e dos titulares.

A implementação da anonimização deve, portanto, ser compreendida como uma estratégia de mitigação de riscos e proteção da privacidade, e não como uma nova operação de tratamento de dados, sendo crucial que o Estudo esclareça adequadamente as diferenças entre as duas atividades, a fim de não confundir os agentes de tratamento.

contato@bbladv.com.br
www.bbladv.com.br

(c) Possibilidade de identificação do titular por terceiros com acesso aos dados anonimizados

Diante da impraticabilidade da ausência completa do risco de reidentificação do titular do dado anonimizado, é importante abordar no Estudo Técnico a possibilidade de identificação do titular por indivíduos que possuem informações adicionais do titular ou por meio do acesso a informações do titular disponíveis publicamente.

Isso porque em alguns casos, o conhecimento pessoal de determinado indivíduo sobre o titular do dado anonimizado poderá possibilitar a identificação do dado anonimizado. A título de exemplo, um médico pode ser capaz de identificar um dos seus pacientes ao ler um estudo anônimo em uma revista médica, ou os residentes de determinada região podem ser capazes de identificar os indivíduos a quem se referem as informações anônimas de um crime ocorrido na localidade.

Adicionalmente, a identificação do titular poderá ocorrer através da correspondência de diferentes conjuntos de dados, de modo que os agentes de tratamento devem considerar quais outros dados do titular podem estar disponíveis publicamente, ou os grupos que provavelmente terão acesso a dados anonimizados, e que podem tornar possível a identificação do titular. Essas informações podem incluir, por exemplo:

- Registros públicos acessíveis pelos membros de determinadas instituições;
- Informações disponibilizadas na internet ou em bases de dados digitais, como matérias de jornais, postagens em *blogs* ou em diretórios *online*;
- Dados estatísticos publicados em formato anonimizado, que podem ser combinados com determinados dados anonimizados para identificar o titular;
- Informações disponíveis para uma organização ou um indivíduo específico ao qual é concedido acesso aos dados anonimizados.

Sugerimos, portanto, a inclusão da possibilidade de identificação de dados anonimizados a partir de informações pessoais em posse de terceiros, bem como pelo cruzamento de dados do titular disponíveis publicamente, a fim de aprimorar a análise do risco de reidentificação e auxiliar os agentes de tratamento na escolha da técnica de anonimização apropriada.

contato@bbladv.com.br
www.bbladv.com.br

(d) Impactos da anonimização aos titulares de dados

Na implementação da anonimização de dados, deve-se ponderar os impactos do emprego desta técnica aos titulares, tendo em vista que, embora as leis de proteção de dados não sejam aplicáveis a estes dados, a utilização de conjuntos de dados anonimizados e disponibilizados para utilização por terceiros pode ocasionar consequências aos titulares.

Desse modo, é necessário cautela no tratamento de informações anonimizadas, especialmente quando essas informações poderão ser utilizadas, muitas vezes em combinação com outros dados, para a tomada de decisões que produzem efeitos sobre os indivíduos, ainda que de forma indireta.

No mesmo sentido, é relevante destacar que o impacto da anonimização sobre os titulares deve ser considerado na avaliação do Risco de Reidentificação Aceitável (RRA). Por exemplo, ao anonimizar dados de saúde de crianças, considerando o longo período de vida desses dados, há alta probabilidade de reidentificação dos titulares nesse espaço de tempo. Assim, é necessário avaliar qual o impacto que, em caso de reidentificação, os titulares dos dados poderiam sofrer nos seus direitos e liberdades. Essa análise deve considerar não apenas a possibilidade de divulgação de dados pessoais sensíveis, mas também todas as consequências futuras para os direitos fundamentais dos titulares caso essas informações sejam acessadas.

Sugerimos, portanto, que o Estudo Técnico aborde a necessidade de os agentes de tratamento analisarem as implicações do uso de técnicas de anonimização e pseudonimização aos titulares de dados, garantindo que o processo adotado atenda ao seu propósito sem comprometer as garantias e os direitos dos titulares.

CONSULTA DE PSEUDOANONIMIZAÇÃO E ANONIMIZAÇÃO – AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

1. Processo de Anonimização - Reidentificação

O estudo técnico traz, na Figura 2, as etapas essenciais para a gestão do risco de reidentificação, sendo sua etapa 4 determinada “acompanhamento do risco de reidentificação”. A nosso ver, a ANPD deveria orientar de forma mais objetiva as boas práticas para realização da revisitação, levando em consideração critérios que possam ser adaptados a diferentes contextos, setores e diferentes níveis de robustez operacional, tecnológica e financeira dos agentes de tratamento.

Ainda no que tange à possibilidade de reidentificação, a ANPD deveria divulgar orientações a serem seguidas pelos agentes de tratamento em casos nos quais eles identifiquem a ocorrência de reversibilidade de dados anonimizados, com objetivo de que tais medidas sejam implementadas nos seus procedimentos a serem estruturados. Por exemplo, seria importante ter a orientação sobre a necessidade de informação ao titular pelo agente de tratamento no caso de reidentificação.

Além disso, deve ser reavaliada a obrigatoriedade de intervenção humana no processo de anonimização, sendo facultado às empresas decidirem qual a melhor abordagem com base em sua avaliação de risco e operações internas.

2. Processo de Anonimização – Modelo baseado em riscos

Acerca do “modelo baseado em riscos para a anonimização”, entendemos que a estruturação de um procedimento robusto para avaliar e prevenir tais riscos de reversibilidade dos dados é inerente a cada agente de tratamento de forma individual, observando-se a sua estrutura tecnológica, financeira, operacional e a natureza dos dados objeto da anonimização. Assim, a ANPD deveria dar mais transparência a eventuais diferenças de avaliações de tais procedimentos e aplicação de medidas considerando tais critérios, reconhecendo a existência de boas práticas atreladas a diferentes setores, e estabelecendo parâmetros mínimos a serem observados.

3. Processo de Anonimização - Tratamento

Considerando o processo da anonimização ser a retirada de identificadores que possam identificar a pessoa natural, questiona-se a aplicação da LGPD ao seu processo inicial, haja vista a sua unicidade de tratamento. Anonimizar é eliminar. É uma operação única. Se a intenção é mencionar o tratamento anterior à anonimização, recomendamos deixar a premissa mais clara, na medida que a afirmação “o ato inicial do processo de anonimização configura operação de tratamento de dado pessoal, atraindo, assim, a aplicação de princípios e regras da LGPD” traz a conotação de o ato inicial do processo de anonimização. O tratamento para o qual o agente de tratamento legitima o seu tratamento e o tratamento da anonimização (eliminação de identificadores) são dois processos distintos.

4. Transparência ao Titular – Anonimização

A autoridade deveria se manifestar mais detalhadamente sobre direitos do titular no que se refere à anonimização dos dados. Cita-se, no estudo, que se deve informar ao titular a intenção de anonimizar o dado no ato inicial da coleta dele, quando tal informação for, de início, sabida pelo agente. Porém, quando a anonimização é decidida posteriormente, deveria ser informado o titular de tal modificação? Poderia o titular se opor à anonimização de seus dados, mesmo quando o agente de tratamento

obedeceu a todas as obrigações relacionadas ao tratamento precedido à anonimização desejada? Entendemos, nesse ponto, que se o tratamento que antecedeu está de acordo com a norma, a anonimização não requer informação posterior ao titular, ou qualquer exercício de direitos, tendo em vista o dado anonimizado não ser mais um dado pessoal e, portanto, a este não mais se aplicaria a LGPD.

TOMADA DE SUBSÍDIOS Nº 01

O objetivo da presente Consulta é receber contribuições de profissionais da área, dos agentes de tratamento, de titulares, do setor acadêmico e da sociedade em geral, de modo a permitir uma atuação regulatória alinhada às melhores práticas e à realidade no que tange aos padrões e técnicas utilizados em processos de anonimização, nos termos do artigo 12, § 3º, da Lei n° 13.709, de 14 de agosto de 2018 (LGPD).

Neste sentido a tomada de subsídios traz a apresentação do estudo preliminar sobre Anonimização e Pseudonimização para a proteção de dados pessoais em que pretendesse manter sua postura estratégica de promover na sociedade brasileira maior efetividade do regime de proteção de dados pessoas através da exposição de algumas bases para a expansão das orientações da ANPD para fortalecer a cultura e a proteção de dados pessoais.

Primordial destacar a diferença existente entre ambos os processos. A anonimização é a 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. Já a pseudonimização de dados pessoais significa substituir quaisquer características identificáveis dos dados por um pseudônimo, ou seja, um valor que não permite a identificação direta do titular dos dados.

Desta forma, a partir das considerações sobre a anonimização e a pseudonimização de dados pessoais apresentadas no **"Estudo Preliminar - Anonimização e pseudonimização para proteção de dados"** entendemos que, os cuidados que devemos ter em ambas as práticas precisam estar bem delineados uma vez que ambos traduzem práticas importantes, em que pese diferentes, para proteção da privacidade das informações pessoais.

Desta forma listamos algumas práticas no intuito de contruibuir sobre os cuidados precisam ser levados em consideração no processo de:

1. Anonimização de Dados:

a) Definição de Objetivos Claros: Antes de iniciar o processo de anonimização, é crucial entender os objetivos e as razões para a realização dessa prática.

b) Avaliação de Riscos Residuais: Certificar-se de avaliar os riscos residuais para garantir que os dados não possam ser revertidos para identificar os indivíduos, ou o que poderá ser feito para minimizar este risco.

c) Métodos Adequados: Utilização de métodos robustos e atualizados para anonimizar dados, como a remoção de informações identificáveis ou a substituição por códigos irreversíveis.

d) Monitoramento Contínuo: Implementação de um sistema de monitoramento contínuo para verificar se os dados permanecem anonimizados ao longo do tempo.

e) Documentação Adequada: Manter registros detalhados do processo de anonimização, incluindo as técnicas utilizadas, para garantir transparência e conformidade.

2. Pseudonimização de Dados:

a) Escolha de Pseudônimos Adequados: Ao criar pseudônimos, evitar informações que possam ser facilmente associadas aos indivíduos, garantindo um nível adequado de proteção.

b) Controle de Acesso: Implementar medidas rigorosas de controle de acesso para garantir que apenas as pessoas autorizadas tenham acesso aos dados pseudonimizados.

c) Atualização Regular dos Pseudônimos: Considerar a possibilidade de atualizar periodicamente os pseudônimos para evitar possíveis correlações com informações externas.

d) Proteção de Chaves de Pseudonimização: Mantenher as chaves de pseudonimização em locais seguros e restritos, garantindo que apenas pessoal autorizado tenha acesso.

e) Avaliação de Impacto na Privacidade: Realizar uma Avaliação de Impacto na Privacidade para entender e mitigar os riscos associados à pseudonimização.

f) Conformidade com Regulamentações: Ciência sobre as regulamentações locais e globais de proteção de dados e certifique-se de que as práticas de pseudonimização estejam em conformidade.

Além destes cuidados podemos citar, para ambas as técnicas, a necessidade de, uma vez que há os procedimentos de anonimização e/ou pseudonimização instituídos: a) Treinamento e Conscientização: Treinar os colaboradores sobre a importância da anonimização e pseudonimização e promova a conscientização sobre práticas seguras; b) Transparência com os Indivíduos: Informar os indivíduos sobre as práticas de anonimização e pseudonimização, garantindo transparência e construindo confiança; e, c) Revisões Periódicas: Realizar revisões periódicas das práticas de anonimização e pseudonimização para garantir que estejam alinhadas com as melhores práticas e regulamentações em evolução.

Tendo em vista que o Estudo Preliminar demonstrou que a anonimização se desenvolve em uma série de etapas que se inicia com o processamento de dados pessoais e tem o objetivo de, com a aplicação de técnicas variadas, desassociar identificadores do dado em seu estado originário ou bruto, imprescindível se faz adotar uma uma abordagem ampla baseada em processo.

Em que pese cada organização seja única, o que equivale dizer que, cada uma delas deve utilizar os mecanismos e técnicas que sejam apropriadas para as suas circunstâncias, isso não exime a Autoridade Nacional de Proteção de Dados (ANPD) do seu dever de regulamentar. Ou seja, estabeleceler um processo base através do qual se originam as técnicas para que a anonimização e a pseudonimização sejam executadas pelas organizações, inclusive a partir das contribuições e dos guias explicativos publicados através da presente tomada de subsídios.

Frisa-se que os guias orientativos possuem uma finalidade educativa, o que torna a necessidade regulamentar ainda maior para que possua força vinculante e possa ser utilizada como fundamentos para resolução dos eventuais incidentes que envolvam um caso concreto.

No que diz respeito ao **“Estudo técnico sobre anonimização de dados na LGPD: Uma visão de processo baseado em risco e técnicas computacionais”**, fica posto que na anonimização de dados não há técnica com eficácia plena, estando todas elas

sujeitas a ataques de reidentificação, isto é, riscos de reidentificação e, por esse motivo, a anonimização deve ser entendida como um processo contínuo baseado em riscos, composto por muitas fases e com transições multidirecionais entre essas, havendo inclusive a possibilidade de o processo de anonimização ser revertido por ação de agentes terceiros ou de agentes internos, não sendo factível considerar que o processo de anonimização pode resultar em um cenário de risco zero.

O risco associado à reversibilidade do processo de anonimização é um elemento chave que deve ser considerado pelo agente de tratamento ao realizar a anonimização dos dados pessoais e, por esse motivo, contribuímos com algumas medidas que sustentam o objetivo principal de reduzir significativamente o risco de reidentificação através de uma abordagem holística (conjunto de dados e as ameaças potenciais):

a) Avaliação de Riscos Iniciais: Antes de aplicar técnicas de anonimização, se faz importante uma avaliação de riscos inicial para identificar os potenciais pontos de reidentificação.

b) Remoção de Identificadores Diretos: Certificar-se de remover identificadores diretos, como nomes, endereços e números de identificação, a fim de garantir que não haja informações explícitas que possam vincular os dados a uma pessoa específica.

c) Generalização de Dados: Generalizar as informações para torná-las menos específicas. Por exemplo, substituir valores exatos por intervalos ou categorias amplas. Isso reduzirá a precisão dos dados, tornando a reidentificação mais difícil. O que já foi apontado no presente estudo.

d) Ruído Adicional (Perturbação): Adicionar “ruídos” aos dados, introduzindo pequenas alterações aleatórias. Essa perturbação dificulta a correspondência exata entre registros e reduz a chance de reidentificação. O que já foi apontado no presente estudo.

e) Amostragem Aleatória: Utilizar uma amostragem aleatória para distorcer ainda mais a correspondência entre dados e indivíduos. Ao selecionar uma amostra representativa, acabamos dificultando a identificação de registros específicos.

f) Preservação da Distribuição Estatística: Ao realizar anonimização, é importante preservar a distribuição estatística dos dados para garantir que as características gerais dos dados permaneçam semelhantes, mas torna mais difícil a reidentificação de indivíduos específicos.

g) Agrupamento: Agrupar valores semelhantes para criar grupos. Isso ajuda a obscurecer dados individuais, pois os registros compartilham características semelhantes dentro dos grupos.

h) Limitação de Dados Disponíveis Publicamente: Evitar divulgar ou publicar dados muito específicos, especialmente quando há combinação com outras fontes de dados públicos que podem facilitar a reidentificação.

i) Uso de Técnicas Avançadas: Considerar a aplicação de técnicas avançadas, como diferenças estatísticas controladas, para garantir a eficácia da anonimização, especialmente em conjuntos de dados complexos.

j) Monitoramento Contínuo: Estabelecer um sistema de monitoramento contínuo para avaliar o risco de reidentificação ao longo do tempo. Isso é crucial, pois as ameaças e técnicas de reidentificação podem evoluir.

k) Testes de Segurança: Realizar testes de segurança regulares para identificar possíveis vulnerabilidades nas práticas de anonimização.

É a contribuição.

SOLINTEL - SOLUCOES INTELIGENTES EM TELECOMUNICACOES LTDA
CNPJ nº 08.429.293/0001-39

CONTRIBUIÇÕES À CONSULTA PÚBLICA SOBRE ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO PARA A PROTEÇÃO DE DADOS PESSOAIS

São Paulo, 14 de março de 2024.

Prezada **Diretoria de Normatização da Autoridade Nacional de Proteção de Dados - ANPD**
normatizacao@anpd.gov.br

Ref.: Consulta à Sociedade de Estudo Preliminar sobre Anonimização e pseudonimização para proteção de dados

Venho, em nome da **Associação Brasileira de Planos de Saúde - ABRAMGE** e da **Associação Brasileira de Planos Odontológicos - SINOG**, na figura de sua Advogada e Encarregada de Proteção de Dados, parabenizar esta autoridade pela excelente condução do tema por intermédio de estudo preliminar, possibilitando à sociedade a participação na construção e maturação da cultura de proteção de dados no Brasil, e também pela importância dada ao tema, a ponto de deliberarem pela aprovação de concessão de prazo adicional para participação social.

Importante reforçar que sinalizamos, tempestivamente na página "Participa + Brasil" voltada à recepção de contribuições à consulta pública, que encaminharíamos nossas contribuições via e-mail (lgpdsistema@abramge.com.br), em virtude da restrição de caracteres (300) dos campos destinados à consulta pública. De tal modo, o fazemos em obediência à orientação da própria ANPD, no item 2 "gostaria de deixar algum comentário ou sugestão adicional?".

Cabe mencionar que o setor de saúde e odontologia suplementares, especialmente as associadas das entidades ABRAMGE e SINOG, acompanha de perto as atividades desta autoridade, sempre que possível contribuindo com as participações sociais propostas pela ANPD, com a ajuda das construções de diversos Grupos de Trabalho sobre o tema.

Deste modo, aproveitamos a oportunidade concedida para destacar os principais pontos de preocupação deste setor em relação ao estudo realizado, com foco nas necessidades da operação junto aos titulares de dados pessoais, conforme expomos a seguir.

I. Ato de anonimizar como operação de tratamento

Quanto ao item 12 da minuta do guia, que trata do art. 5, III, da LGPD, opinamos que se um processo for divulgado de forma anonimizada, deve-se dispor sobre a necessidade de mapeamento e aplicação da base legal antes da técnica de anonimização.

O Guia (parágrafo 29) enfatiza que o ato inicial de anonimização configura uma operação de tratamento de dados pessoais, sujeitando-se, portanto, à Lei Geral de Proteção de Dados (LGPD). Nesse sentido, o Guia ressalta alguns requisitos de legalidade para esse tipo de atividade de tratamento: a existência de base legal (parágrafo 21), a informação prévia ao titular sobre a anonimização (parágrafo 33) e a atenção aos princípios previstos na LGPD, especialmente os da finalidade, da necessidade e da adequação (parágrafo 32). Além disso, o Guia também explicita que a origem dos dados pessoais deve ser lícita e que a anonimização não tem a capacidade intrínseca de legitimar atividades de tratamento inicialmente ilícitas. Em termos práticos, isso significa que a anonimização não pode transformar, por si só, uma atividade de tratamento de dados pessoais sem base legal em uma prática legítima. As posições destacadas no Guia baseiam-se, em essência, nas referências europeias sobre o tema, especialmente no Parecer 05/2014 sobre técnicas de anonimização do Grupo de Trabalho de Proteção de Dados do Artigo 29.

No que diz respeito à licitude da origem e da impossibilidade de validação, por meio da

anonimização, de dados que tenham sido ilicitamente coletados, não nos parece haver argumento contrário razoável do ponto de vista dos preceitos da proteção de dados. No entanto, quanto à consideração da anonimização como uma operação de tratamento autônoma sujeita à integralidade das exigências da LGPD e à imposição de limitações ao uso dos dados já anonimizados, há contrapontos relevantes a serem apresentados, especialmente considerando o avanço tecnológico que impacta o uso de dados pessoais anonimizados. Nesse contexto, é importante considerar a realidade associada à formação de *data lakes* e o avanço da inteligência artificial, fatores que não foram enfrentados pelo regulador europeu no tempo de emissão do parecer referenciado pela Autoridade brasileira.

Nesse novo cenário se faz mandatório considerar que a rigidez na exigência de finalidade específica e necessidade bem definidas para a anonimização pode inviabilizar atividades relevantíssimas do ponto de vista tecnológico e econômico. A dinâmica complexa e interconectada dos *data lakes* e a natureza exploratória da inteligência artificial encontram obstáculo em tais limitações, já que estão associadas a derivações e à descoberta de novas utilidades, ações que podem ser legítimas às organizações e não necessariamente prejudiciais aos titulares. Isso, por si, pode demandar uma revisão das práticas de anonimização, visando conciliar a proteção da privacidade com a flexibilidade necessária para o avanço tecnológico.

Esses aspectos colocam em xeque as exigências de definição de base legal, de informação prévia ao titular e da aplicação do uso secundário, como sugerido pelo Guia (parágrafo 37). Uma sugestão relevante a ser considerada é a abordagem que reconheça a anonimização como uma finalidade autônoma. Tal implica em conceber a anonimização não apenas como um meio para alcançar outros fins, mas, sim, como um objetivo independente e válido por si só. Ao adotar essa perspectiva, a anonimização seria tratada como uma finalidade intrínseca ao tratamento de dados, não meramente como um meio para outros propósitos. Alternativamente, seria benéfico o reconhecimento, pela ANPD, de categorias mais abrangentes de finalidades associadas às necessidades do contexto de desenvolvimento tecnológico atual. Por exemplo, considerando a formação de *data lakes* e as análises exploratórias de dados, poderia se estabelecer categorias amplas que englobassem essas atividades e outras práticas similares.

Em mesma linha, seria conveniente que fossem consideradas pela ANPD:

(i) a dispensa de base legal para o ato de anonimização; ou

(ii) para fins de uso secundário, a atribuição de uma presunção de compatibilidade ao ato de anonimização (tanto no caso da anonimização como finalidade autônoma, quanto as de finalidades abrangentes associadas à anonimização, citadas no parágrafo acima).

Nesses cenários, caso o tratamento original dos dados tenha sido conduzido de maneira estritamente lícita e as técnicas de anonimização empregadas sejam comprovadamente eficazes, não representando riscos relevantes aos titulares, seria positivo ao agente de tratamento não se ver obrigado a buscar uma base legal adicional.

Por fim, não se pode ignorar que a vinculação da anonimização a finalidades específicas significa limitar atividades que estão reconhecidamente fora do escopo de aplicação da LGPD. É, inclusive, o que faz o Guia (parágrafo 54) ao prever que os dados anonimizados apenas podem ser utilizados para finalidades compatíveis com aquelas para as quais os dados pessoais originais foram coletados. Na prática, a adoção do referido posicionamento significa regulação de atividades fora da aplicação da LGPD. Não há justificativa razoável para tal restrição, que significaria uma expansão por via infralegal da aplicação da própria LGPD.

Ponto	**Sugestão**
Aplicação dos Princípios da finalidade, da necessidade e da adequação (parágrafos 32 - 40).	Considerar a anonimização como uma finalidade autônoma; ou criar categorias mais abrangentes

	de finalidades associadas às necessidades do contexto de desenvolvimento tecnológico (*e.g.* formação de *data lakes* e análises exploratórias).
Existência de base legal (parágrafo 21) / Aplicação do uso secundário (parágrafo 37).	Dispensa de base legal para o ato de anonimizar quando o tratamento original for lícito e as medidas de anonimização sejam eficazes; ou conferir presunção de compatibilidade para finalidade de anonimização (ou para as finalidades abrangentes citadas no item acima).
Informação prévia ao titular (parágrafo 33).	A previsão deve ser considerada como boa prática, não como mandatória.
Limitação às novas finalidade para o uso de dados anonimizados (parágrafo 54).	Não prever limitação de compatibilidade para o uso de dados anonimizados.

II. Anonimização como uma medida de segurança não impositiva

O Guia expõe no parágrafo 40 que "a anonimização não é uma medida de segurança impositiva, que deve ser adotada em todo e qualquer tratamento de dados pessoais" e que a adoção (ou não) de técnicas de anonimização decorre de um juízo de necessidade pelo agente de tratamento em face da(s) finalidade(s) especificada(s) para o tratamento de dados na situação concreta.

O ICO (*Information Commissioner's Office*)[11], autoridade britânica de proteção de dados pessoais, que é um importante parâmetro internacional, afirma que a utilização de dados pessoais é legítima para determinados fins. Em algumas situações, para alcançar a finalidade pretendida, pode ser que o agente de tratamento deva necessariamente tratar dados pessoais, como é o caso, por exemplo, da prestação de serviços a determinados indivíduos ou a realização de pesquisas médicas que envolvem o tratamento de dados pessoais de pacientes e são realizadas com base na participação e concordância destes pacientes.

Outra referência internacional relevante no que diz respeito à interpretação dos institutos de proteção de dados pessoais, a PDPC (*Personal Data Protection Commission*), autoridade de Singapura, por meio do *Advisory Guidelines on the Personal Data Protection Act for Selected Topics*[22] publicado em setembro de 2013 e revisto em maio de 2022, entende que:

"A natureza do conjunto de dados afeta a quantidade de informações identificáveis que precisam ser removidas para que não possam mais ser usadas para identificar indivíduos. Alguns tipos de dados são inerentemente 'ricos' e repletos de informações [...], de modo que qualquer alteração para anonimizar os dados pode torná-los inúteis para seus propósitos pretendidos." [33]

1 INFORMATION COMMISSIONER'S OFFICE. **Introduction to anonymisation: Draft anonymisation, pseudonymisation and privacy enhancing technologies guidance.** Acesso em: fev/2024. Disponível em: https://ico.org.uk/media/about-the-ico/consultations/2619862/anonymisation-intro-and-first-chapter.pdf

2 PERSONAL DATA PROTECTION COMMISSION. **Advisory Guidelines on the Personal Data Protection Act for Selected Topics**. Acesso em: fev/2024. Disponível em: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Selected-Topics/Advisory-Guidelines-on-the-PDPA-for-Selected-Topics-17-May-2022.pdf

3 O subcapítulo 3.1.3 do Guia trata dos conceitos de esforços razoáveis e meios próprios previstos no artigo 12 da LGPD: "Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido".

Em outras palavras, a disposição estabelecida pelo Guia de que o processo de anonimização não pode ser obrigatório é positiva, devendo ser uma recomendação ao agente de tratamento para a proteção dos dados, uma vez que, como bem explicitado pelas autoridades britânica e singapurense, há situações na qual o tratamento de dados pessoais é necessário para o alcance da finalidade pretendida pelo agente de tratamento.

Ponto	**Sugestão**
A anonimização não é uma medida de segurança impositiva (parágrafo 40).	Ressaltar sua manutenção no Guia. A disposição é positiva, considerando que não pode haver ao agente de tratamento a obrigação de anonimizar. A previsão deve ser considerada como boa prática do agente de tratamento, não como mandatória.

III. Risco de reidentificação

O Guia enfatiza no parágrafo 42 que, de acordo com o atual estado da arte, pode-se concordar com a existência de um consenso científico sobre a impraticabilidade de um cenário de ausência de risco de reidentificação de dados anonimizados. Também afirma que sempre existirá o risco de reidentificação dos dados anonimizados, diante do enorme volume de dados auxiliares disponibilizados publicamente na internet e o desenvolvimento da capacidade de processamento e análise de algoritmos de reidentificação.

A interpretação acolhida pela ANPD no Guia, a nosso ver, é positiva e se trata de um entendimento mais moderno em relação ao processo de anonimização, levando em conta que nenhuma técnica de anonimização é capaz de garantir a impossibilidade absoluta de reidentificação dos dados anonimizados. Isso porque, diante do cenário atual, sempre haverá o risco de reversão da anonimização, independente da técnica utilizada pelo agente de tratamento.

Ponto	**Sugestão**
Impraticabilidade de um cenário de ausência de risco de reidentificação de dados anonimizados. Sempre haverá fatores de risco de reidentificação (parágrafo 42).	Ressaltar sua manutenção no Guia. A posição adotada é positiva e deve ser mantida, na medida em que, conforme exposto acertadamente no Guia, não há nenhuma técnica de anonimização que seja absoluta e apresenta risco zero de reidentificação do dado anonimizado.

IV. Modelo baseado em riscos

Diante da impossibilidade de um cenário de risco zero de reidentificação, o Guia considera a adoção de um modelo baseado em riscos (parágrafo 43) no que diz respeito à identificabilidade dos dados, segundo os meios e esforços razoáveis, para avaliar a eficácia e a robustez de uma anonimização. Também nesse sentido, o Guia delineia que o agente de tratamento deve realizar esta avaliação, não de modo pontual e episódico, mas, sim, de forma iterativa e contínua.

No que diz respeito à primeira parte do parágrafo 43, entendemos que a adoção de um modelo baseado em riscos para avaliar o processo de anonimização é adequado e passível de ser aplicado pelos agentes de tratamento em um contexto prático. Por outro lado, é importante ter em conta que a análise dos riscos relacionados às técnicas de anonimização tem suas limitações e que a continuidade e a iteratividade também apresentam restrições. Para tanto, é importante que a aplicação do modelo de riscos seja aplicada considerando o esforço razoável do controlador para aferir riscos e manter a continuidade e iteratividade.

Ponto	**Sugestão**
Modelo baseado em riscos para avaliar o processo de anonimização (parágrafo 43 - primeira parte).	Ressaltar sua manutenção no Guia. O modelo baseado em riscos sugerido pela ANPD é adequado, uma vez que considera os meios e esforços suscetíveis de serem razoavelmente utilizados pelo agente de tratamento.
Avaliação do processo de anonimização de forma iterativa e contínua (parágrafo 43 - segunda parte).	É importante que se considere que a iteratividade e a continuidade desta avaliação também têm suas limitações, ou seja, deve haver um esforço razoável do controlador, na medida dos meios disponíveis a ele.

V. Noções de esforços razoáveis e meios próprios

O Guia sinaliza que o instituto dos "esforços razoáveis" deve ser entendido como um conceito jurídico indeterminado, o que significa que sua definição depende da avaliação subjetiva do aplicador do Direito. A ANPD, como órgão interpretativo e fiscalizador da LGPD, deve preencher esse conceito considerando elementos pertinentes ao caso específico, conforme estabelecido no § 1º do artigo 12.

O Guia ressalta que a LGPD oferece uma lista exemplificativa de aspectos objetivos a serem considerados ao definir o que são "esforços razoáveis". Esses aspectos incluem custo e tempo necessários para reverter o processo de anonimização, com base nas tecnologias disponíveis, e a utilização exclusiva de meios próprios. Por exemplo, na avaliação dos custos e tempo para a reidentificação dos dados, deve-se levar em conta os recursos humanos e econômicos necessários, conforme destacado em uma Nota Técnica da ANPD envolvendo o tratamento de microdados pelo INEP. Outros fatores objetivos importantes incluem as tecnologias e técnicas disponíveis no momento do tratamento, bem como a licitude dos meios utilizados. Isso implica que o uso de meios proibidos por lei para reidentificação configura esforços irrazoáveis.

Meios próprios, por sua vez, pelo entendimento descrito no Guia, seriam tanto as habilidades, os dados, instrumentos e técnicas disponíveis ao próprio agente de tratamento responsável pela anonimização, quanto a atuação de outras pessoas ou entidades que, com meios e esforços razoáveis, podem reidentificar conjunto de dados anonimizados. Aqui cabe destacar que a ANPD sugere uma interpretação específica ao termo “próprios” previsto na LGPD, entendendo que o termo faz referência à titularidade (ou propriedade) dos meios referidos acima. Levando em consideração o conteúdo dos Estudos, a ANPD distingue duas abordagens possíveis para essa questão: (i) relativa ou subjetiva, na

qual apenas se considera os esforços individuais e os meios próprios do agente de tratamento responsável pela anonimização dos dados, não levando em conta a atuação de outros indivíduos ou entidades; e (ii) absoluta ou objetiva, na qual se considera o potencial de identificação não apenas pelos esforços do responsável pelo tratamento, mas também por qualquer outros terceiros. Em conclusão, no Guia, a ANPD privilegia a abordagem absoluta ou objetiva.

As posições destacadas acima baseiam-se, essencialmente, nas referências europeias sobre o tema, especialmente no texto da revogada Diretiva n. 95/46/CE ou do vigente Regulamento n. 2016/679. No que diz respeito à noção de esforço razoável como um conceito jurídico indeterminado, não nos parece haver argumento contrário à interpretação dada pela Autoridade. Por outro lado, em relação à adoção de uma perspectiva absoluta ou objetiva para o conceito de meios próprios empregado pela ANPD, há contrapontos a serem apresentados.

Uma vez que a Autoridade confere ao termo "meios próprios" a interpretação no sentido narrado acima, de considerar os meios do próprio controlador, não nos parece haver espaço para aplicação da abordagem objetiva. Tal seria, em essência, uma contradição à disposição legal. Se a Lei determina que sejam considerados os meios do próprio controlador, haveria flagrante contradição em se contemplar a capacidade de terceiros na reversão da anonimização. Ainda sobre esse ponto, é também fundamental considerar as limitações que o próprio controlador tem em relação à capacidade de reversão da anonimização que terceiros estranhos à sua cadeia de tratamento sob sua responsabilidade possam ter. Por isso, nos parece que a abordagem relativa ou subjetiva é aquela definida pelo mandamento legal do artigo 12 da LGPD.

Para que a abordagem absoluta ou objetiva tivesse sentido no contexto brasileiro, a ANPD teria de conferir outra interpretação ao conceito de "meios próprios". Para tanto, um caminho possível seria o de não considerar o fator objetivo de licitude como um elemento de esforço razoável, mas, sim, como um requisito para que os meios sejam considerados próprios. Ou seja, meios próprios seriam os meios lícitos, em contraposição aos impróprios, que seriam aqueles meios ilícitos. Por essa perspectiva, ao aferir se a anonimização é reversível, o controlador deveria ponderar os meios, sejam de sua titularidade e de terceiros, que fossem lícitos e que tivessem condão de reverter o processo. Esta é a abordagem interpretativa que, preservando o sentido lógico e o alinhamento à disposição da LGPD, poderia exigir que os meios de terceiros fossem considerados na avaliação da reversibilidade da anonimização.

Em resumo, do ponto de vista prático para os agentes de tratamento, entendemos que o mais adequado para o Guia é a previsão de que o controlador deve considerar a capacidade, unicamente através de meios lícitos, de reidentificação por si ou por terceiros legitimamente envolvidos na cadeia de tratamento (*e.g.* outro agente de tratamento para o qual os dados anonimizados foram legalmente transferidos mediante acordo de tratamento).

Ponto	**Sugestão**

Meios próprios abrangem as habilidades, os dados, instrumentos e técnicas disponíveis ao próprio agente de tratamento responsável pela anonimização e a terceiros (parágrafo 52).	A interpretação dada pela ANPD no Guia em relação ao conceito de meios próprios adotou essencialmente uma perspectiva absoluta ou objetiva, considerando tanto os meios disponíveis ao próprio agente de tratamento quanto a outras pessoas ou entidades. A nosso ver, a noção de meios próprios deve adotar uma perspectiva relativa ou subjetiva, de forma que sejam considerados unicamente os meios próprios disponíveis ao agente de tratamento responsável pelo processo de anonimização. E, em última instância, dos terceiros legitimamente associados à cadeia de tratamento. Em resumo, do ponto de vista prático para os agentes de tratamento, entendemos que o mais adequado para o Guia é a previsão de que o controlador deve considerar a capacidade, unicamente através de meios lícitos, de reversão da identificação por si ou terceiros legitimamente envolvidos na cadeia de tratamento.

VI. Utilidade dos dados

O Guia (parágrafo 58) indica que cabe ao controlador identificar o grau de utilidade dos dados anonimizados, e, em consequência, estabelecer o grau necessário de anonimização. Para tanto, o Guia também considera que a anonimização não torna os dados inúteis, mas mantém os dados funcionais para um determinado propósito de tratamento e finalidades específicas.

Reconhecer a utilidade dos dados anonimizados e considerá-la no processo de anonimização é fator positivo para os agentes de tratamento. No entanto, vincular a utilidade de dados anonimizados a finalidades específicas, tal qual se exige dos dados pessoais, é medida inadequada, do mesmo modo do indicado no item I deste documento. Após a submissão dos dados a um processo eficaz de anonimização, estes não serão mais considerados dados pessoais, nos termos do artigo 12 da LGPD, de forma que as disposições da Lei, neste caso a exigência de finalidade, não seriam aplicáveis aos dados anonimizados.

Ponto	**Sugestão**
A anonimização não torna os dados inúteis (parágrafo 58).	Ressaltar sua manutenção no Guia. A interpretação adotada no Guia de que a anonimização não torna os dados inúteis é positiva. É fundamental que a ANPD considere esta ponderação, de que os dados anonimizados devem manter sua utilidade e que ela seja considerada na avaliação de risco para caracterização da anonimização.

Um processo adequado de anonimização mantém os dados funcionais para um determinado propósito de tratamento e finalidades específicas (parágrafo 58).	O parágrafo 58 dispõe a respeito da finalidade do tratamento de dados pessoais, entretanto, como defendemos no item I, a vinculação da anonimização a finalidades específicas significa a regulação de atividades fora da aplicação da LGPD. Isso porque os dados anonimizados não são considerados dados pessoais e seu uso não exige finalidade definida. Desse modo, a exigência de uma finalidade específica, no que diz respeito a dados anonimizados, significaria uma expansão por via infralegal do que dispõe a própria LGPD.

VII. Metodologia do processo de anonimização baseado em risco

Inicialmente, o Guia expõe no subcapítulo 3.2.2 "Gestão do risco de reidentificação" (parágrafos 61 e 62) que o processo de anonimização não pode ser entendido como um processo definitivo e que não há técnica de anonimização de eficácia plena que apresenta risco zero de reidentificação dos dados. Isto é, a anonimização tem como objetivo minimizar os riscos de reidentificação dos dados mantendo a utilidade dos dados anonimizados.

No que diz respeito a esse ponto, a nosso ver, como exposto acima no item VII, o Guia, acertadamente, explicitou que nenhum processo de anonimização é plenamente eficaz e que em nenhuma situação haverá risco zero de reidentificação dos dados submetidos à anonimização, cabendo ao agente de tratamento gerenciar os riscos residuais na medida dos meios disponíveis a ele.

Os demais parágrafos do subcapítulo oferecem uma proposta de processo de anonimização baseado em risco, contando com quatro etapas. A primeira etapa visa determinar o Risco de Reidentificação Aceitável (RRA) para um certo conjunto de dados, a fim de estipular um limite superior para o risco. O Guia expõe que um risco de reidentificação superior ao limite estabelecido pelo RRA descaracterizá o conjunto de dados como anonimizado. Sobre isso, o Guia não define uma metodologia padronizada para esta etapa, levando em conta a ampla quantidade de variáveis para as situações concretas (*e.g.* dados sensíveis ou dados financeiros), cabendo ao agente de tratamento definir o RRA para os dados tratados.

A segunda etapa proposta consiste na aplicação do processo de anonimização escolhido pelo agente de tratamento para produzir um conjunto de dados anonimizados com risco de reidentificação não superior ao limite do RRA.

A terceira etapa, por sua vez, visa estabelecer o Risco de Reidentificação Mensurado (RRM) de um ataque de reidentificação ter sucesso nos dados anonimizados. Levando em conta a diversidade de natureza, escopo, contexto e finalidade de cada tratamento realizado pelo agente de tratamento, o Guia não define uma métrica única para o RRM e adota a expressão "Métrica Contextual" para se referir à métrica utilizada para mensurar o RRM que se adapte a realidade de cada agente de tratamento e ao contexto dos dados. A Métrica Contextual baseia-se em métricas de mensuração que utilizam o conceito de equivalência de classe da teoria dos conjuntos para determinar o risco de reidentificação.

O Guia delineia que "*a métrica de risco de reidentificação pode ser computada para cada um dos titulares pertencentes ao conjunto de dados, e os valores resultantes podem ser ponderados, por exemplo, com a média aritmética, para determinar o valor geral da Métrica Contextual. Por fim, o valor geral da Métrica Contextual pode ser então ponderado pelas variáveis*

contextuais, resultando no RRM": Risco de Reidentificação Mensurado = $\boldsymbol{\theta} * \boldsymbol{Vc}$, onde $\boldsymbol{\theta}$ representa o valor geral da métrica contextual e $\boldsymbol{Vc}$ representa um fator de ponderação das variáveis contextuais, quando existentes, e se não existam $\boldsymbol{Vc}$ pode assumir o valor de 1. O RRM deve ser comparado ao RRA e, caso o RRM seja maior do que o RRA, o conjunto de dados não está em condições de ser anonimizado, sendo necessário o reinício do processo de anonimização. Caso contrário, é necessário acompanhar o uso do conjunto de dados, especialmente quando operações realizadas sobre ele possam modificar o risco mensurado.

A nosso ver, houve a proposição de uma metodologia baseada em riscos objetiva (vide o cálculo aritmético) condicionada a uma análise do agente de tratamento de critérios subjetivos, o que gera obstáculos na aplicação prática dos conceitos sugeridos pelo Guia e insegurança aos agentes de tratamento.

Ponto	**Sugestão**
Anonimização considerada como um processo que não é plenamente eficaz e não apresenta risco zero de reidentificação (parágrafos 61 - 62).	A interpretação é positiva e deve ser mantida, na medida em que, conforme exposto acertadamente no Guia, não há nenhuma técnica de anonimização que seja absoluta e apresenta risco zero de reidentificação do dado anonimizado.
Proposta de processo de anonimização baseado em risco. RRA, RRM e Métrica Contextual (parágrafos 63 - 75).	A proposição sugerida pelo Guia no processo de anonimização estipula métodos objetivos a partir de critérios subjetivos, cuja delimitação fica sob responsabilidade do agente de tratamento. Trata-se de cenário de insegurança jurídica aos agentes de tratamento. Caso opte por manter tal metodologia, a ANPD deve precisar a aplicação dos critérios previstos no Guia, para balizar sua devida aplicação prática.

VIII. Avaliação de impacto à proteção de dados

O Guia expõe que, para haver uma metodologia eficaz de pseudonimização, deve ser realizada uma avaliação de impacto sobre a proteção de dados, com a elaboração de um Relatório de Impacto à Proteção de Dados Pessoais (RIPD), quando aplicável, e sempre que o tratamento for de alto risco, objetivando analisar os riscos associados à pseudonimização e garantir a conformidade com a LGPD (parágrafo 84.10).

Entretanto, a nosso ver, a pseudonimização deveria ser uma consequência das conclusões extraídas de um RIPD, em vez de servir como desencadeador para a elaboração desta avaliação. Em outras palavras, o objetivo da pseudonimização não é gerar riscos, mas, sim, atuar como uma medida de mitigação de riscos.

Nesse sentido, o GDPR dispõe, nos Considerandos 28 e 78, respectivamente, que "*a aplicação da pseudonimização a dados pessoais pode reduzir os riscos para os indivíduos envolvidos e ajudar os controladores e operadores a cumprir suas obrigações de proteção de dados*" além de ser considerada como "*uma medida técnica e organizacional apropriada*" (tradução livre). Diante do exposto, entendemos que a elaboração de uma avaliação de impacto não deve antevir a aplicação de um processo de pseudonimização.

Ponto	**Sugestão**
Elaboração de um RIPD anteriormente à aplicação de pseudonimização para análise dos riscos associados a esta prática (parágrafo 84.10).	O objetivo da pseudonimização não é gerar riscos, mas, sim, servir como controle mitigatório, considerando que ela é geralmente adotada como medida de mitigação a partir das conclusões de uma avaliação de impacto. Assim, a elaboração de um RIPD não deve preceder e ser condicionante para a implementação de um processo de pseudonimização.

IX. Comunicação com os titulares

O Guia expõe que, para haver uma metodologia eficaz de pseudonimização, o titular deve ser informado de forma transparente e acessível aos titulares sobre a pseudonimização de seus dados pessoais e os direitos de acesso e correção de suas informações pessoais, conforme exigido pela LGPD (parágrafo 84.11).

No entanto, como expusemos acima no item IX, a pseudonimização é compreendida como uma medida de mitigação que objetiva a minimização de riscos. Ela não tem o condão de gerar riscos adicionais aos titulares de dados. Desse modo, não vemos nenhuma razão para que os titulares sejam informados caso o controlador opte por aplicar técnicas de pseudonimização aos dados pessoais que estão sob sua custódia. O controlador pode optar por descrever no rol de medidas de segurança a respeito da adoção de pseudonimização - como uma medida de boa prática que partiu do próprio agente de tratamento -, e não como uma condicionante para um processo eficaz de pseudonimização.

Ponto	**Sugestão**
Comunicação aos titulares a respeito da	Não há necessidade de comunicação específica

prática de pseudonimização (parágrafo 84.11).	aos titulares sobre a adoção de pseudonimização aos dados pessoais, levando em consideração que a pseudonimização serve como medida de mitigação de riscos e não tem o objetivo de acrescer riscos. Assim, entendemos que o controlador pode optar por detalhar que há pseudonimização no rol de medidas de seguranças adotadas, mas tal condição não pode ser considerada um requisito específico para uma metodologia eficaz de pseudonimização.

Renovando os protestos de elevada estima e consideração, colocamo-nos à disposição para demais informações necessárias e despedimo-nos,

Camila Castioni
OAB 465.457

CAMILA CASTIONI SECUNDINO:45426609829
Assinado de forma digital por CAMILA CASTIONI SECUNDINO:45426609829
Dados: 2024.03.14 19:00:14 -03'00'

São Paulo, 14 de março de 2024.

À AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS ("ANPD")
Coordenação-Geral de Normatização

Ref.: Consulta à Sociedade sobre o Guia de Anonimização e Pseudonimização

A ASSOCIAÇÃO NACIONAL DOS BUREAUS DE CRÉDITO ("ANBC"), pessoa jurídica constituída na forma de associação civil sem fins lucrativos, com sede na Avenida das Nações Unidas, n.º 14.401, Conjuntos 502 e 503, Cidade de São Paulo, Estado de São Paulo, é uma entidade que reúne os bureaus atuantes no território brasileiro, com o objetivo de representar o setor de bureaus de crédito no país, inclusive junto a agentes internacionais, incentivar a educação financeira e colaborar para a criação de um ambiente legal e regulatório que permita à gestão de crédito contribuir ativamente com a economia brasileira.

Em 30 de janeiro de 2024, a ANPD disponibilizou, por meio da Plataforma "Participa + Brasil",[1] Consulta à Sociedade[2] acerca do seu Estudo Preliminar sobre Anonimização e Pseudonimização para Proteção de Dados ("Estudo Preliminar"), a fim de coletar contribuições de profissionais da área, agentes de tratamento, titulares, setor acadêmico e da sociedade em geral. A consulta pretende alinhar a atuação regulatória da Autoridade às melhores práticas em matéria de anonimização e pseudonimização de dados pessoais.

Nessa oportunidade, a ANBC vem apresentar a sua contribuição à ANPD, reiterando seus cumprimentos pela iniciativa de consultar e colher subsídios de todos os setores interessados com vistas a contribuir para a atuação da Autoridade em torno do tema.

* * *

[1] ANPD. "Consulta à Sociedade - Estudo Preliminar - Anonimização e pseudonimização para proteção de dados". Disponível em: <https://www.gov.br/participamaisbrasil/consulta-a-sociedade-estudo-preliminar-anonimizacao-e-pseudonimizacao-para-protecao-de-dados>. Acesso em: 21.02.2024.

[2] ANPD. "ANPD abre consulta à sociedade sobre o Guia de Anonimização e Pseudonimização". Disponível em:<https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-abre-consulta-a-sociedade-sobre-o-guia-de-anonimizacao-e-pseudonimizacao>. Acesso em: 21.02.2024.

ANBC
ASSOCIAÇÃO NACIONAL DOS BUREAUS DE CRÉDITO

CONSIDERAÇÕES SOBRE A MINUTA DO GUIA DE ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO DA ANPD

1. Glossário

Inicialmente, observa-se que o parágrafo 8 do Estudo Preliminar busca apresentar um glossário com conceitos básicos em matéria de privacidade, proteção de dados e anonimização, a fim de auxiliar o leitor na compreensão das orientações da ANPD. Apesar de essa ideia ser interessante para fins de padronizar e de proporcionar um melhor entendimento dos significados dos termos técnicos utilizados ao longo do documento, a ANBC sugere que a Autoridade centre a definição de conceitos no seu Glossário de Proteção de Dados Pessoais e Privacidade.[3]

O Glossário tem por objetivo justamente apresentar o significado dos principais conceitos, termos e expressões usados na Lei Geral de Proteção de Dados Pessoais (Lei Federal n.º 13.709/2018, ou "LGPD") e nos documentos da ANPD, motivo pelo qual se entende que uma atualização constante desse documento garantiria maior uniformidade no entendimento conceitual e técnico da Autoridade. Assim, a ANBC acredita que os termos contidos no parágrafo 8 do Estudo Preliminar poderiam ser apresentados diretamente no Glossário de Proteção de Dados Pessoais e Privacidade da ANPD, reunindo em um único documento o entendimento conceitual e técnico da Autoridade na matéria.

2. Anonimização e os princípios de proteção de dados pessoais

a. Anonimização como atividade de tratamento de dados pessoais

A partir do parágrafo 27 do Estudo Preliminar, especificamente no parágrafo 30, a ANPD parece indicar que a anonimização de dados pessoais seria uma atividade de tratamento (artigo 5º, X, LGPD) em si mesma, com o intuito de desassociar os identificadores que se referem aos titulares dos dados. Ainda que a ANBC compreenda o raciocínio utilizado pela Autoridade, fato é que a anonimização não pode ser entendida meramente como um tratamento, haja vista que a legislação define anonimização como a utilização de meios

[3] ANPD. "ANPD lança Glossário de Proteção de Dados Pessoais". Disponível em:<https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-lanca-glossario-de-protecao-de-dados-pessoais>. Acesso em: 26.02.2024.

técnicos razoáveis e disponíveis no momento de um tratamento específico – que não se trata da anonimização em si –, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo (artigo 5º, XI, LGPD), sem que haja qualquer referência a uma operação posterior com dados. Ao mesmo tempo, a definição de tratamento apresentada pela LGPD indica uma série de atividades, como coleta, utilização, acesso, processamento, armazenamento e eliminação (artigo 5º, X, LGPD), sem qualquer menção à anonimização.

Nesse sentido, a ANBC entende que a anonimização não contrariaria a finalidade inicial do tratamento realizado pelo controlador (conforme disposto no artigo 5º, XI, da LGPD). Isso porque a anonimização ocorreria no momento imediatamente anterior à perda da associação de um dado a um titular, sendo, por esse motivo, plenamente compatível com operações lícitas anteriores. Logo, infere-se que não seria necessário um fundamento jurídico distinto do que permitiu o tratamento inicial dos dados pessoais, como consagra a experiência internacional na matéria: à luz do considerando 50 do Regulamento Geral sobre a Proteção de Dados 2016/679 da Europa ("GDPR"), o tratamento de dados pessoais para outros fins que não aqueles para os quais inicialmente coletados será autorizado quando compatível com as finalidades originais de tratamento, não sendo necessária uma hipótese legal distinta da que permitiu a operação prévia com os dados pessoais. Sob essa lógica, a ANBC defende que a anonimização não dependeria de fundamentação em nova hipótese legal prevista nos artigos 7º ou 11 da LGPD, uma vez que essa obrigatoriedade poderia, em última instância, inviabilizar a anonimização.

No ponto, considerando que ***(i)*** dentre outros objetivos, a LGPD visa proteger as liberdades e os direitos fundamentais dos titulares de dados pessoais; e ***(ii)*** a anonimização consiste na remoção de qualquer possibilidade de identificação de titulares, impedindo a ocorrência de danos e violações aos seus direitos, é possível concluir que dificultar ou inviabilizar a anonimização é, no limite, ir contra um dos objetivos centrais da legislação de proteção de dados. Com efeito, limitar a anonimização e o uso de dados anonimizados não confere aos titulares ou à sociedade qualquer proteção adicional, mas pode representar uma interpretação extensiva da lei, que foi clara ao afastar a aplicabilidade da LGPD aos dados anonimizados.

Com isso em mente, defende-se que a ANPD indique expressamente que a anonimização corresponde a uma medida de segurança a ser implementada pelo controlador, não

significando uma nova atividade que dependa de uma base legal ou que contempla uma finalidade incompatível com o tratamento inicial dos dados pessoais.

b. Utilização posterior de dados anonimizados e princípio da finalidade

A Autoridade afirma, no parágrafo 54 de seu Estudo Preliminar, que os agentes de tratamento podem utilizar dados anonimizados para outras finalidades – desde que compatíveis – além daquelas para as quais as informações tenham sido originalmente coletadas. Todavia, a ANBC entende que a utilização de dados anonimizados não deve atender ao princípio da finalidade, segundo o qual a operação com dados deve se voltar para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades (artigo 6º, I, LGPD).

De fato, após a anonimização, o controlador não precisa garantir a aplicação dos princípios previstos no artigo 6º da LGPD, em relação a qualquer operação realizada com dados anonimizados, uma vez que eles não mais são considerados dados pessoais (artigo 12, LGPD). Esse entendimento é, inclusive, referendado pelo Guidance on Anonymisation and Pseudonymisation,[4] da autoridade de proteção de dados da Irlanda, segundo o qual dados irreversíveis e eficazmente anonimizados não são dados pessoais e os princípios de proteção de dados não precisam ser cumpridos em relação a essas informações. A autoridade da Irlanda indica que o controlador pode, consequentemente, utilizar dados anonimizados para outros fins além daqueles que inicialmente justificaram a coleta das informações.

Nessa linha, o controlador brasileiro é também livre para operar as informações sobre as quais a LGPD não é aplicável, inclusive para finalidades que não sejam compatíveis com o tratamento anterior indicado ao titular, motivo pelo qual a ANBC sugere a revisão do parágrafo 54 do Estudo Preliminar para retirar o trecho, por exemplo, “desde que compatíveis”.

c. Princípio da necessidade e dados anonimizados

[4] Data Protection Comission. “Guidance on Anonymisation and Pseudonymisation”. Disponível em:<https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190614%20Anonymisation%20and%20Pseudonymisation.pdf>. Acesso em: 26.02.2024.

Outro ponto de atenção constante no Estudo Preliminar da ANPD é a argumentação de que, uma vez cumprida a finalidade de tratamento, a retenção das informações para uso exclusivo do controlador só seria possível desde que os dados fossem anonimizados (parágrafo 39 do Estudo Preliminar), observando o princípio da necessidade.

Ocorre que a LGPD, em seu artigo 16, IV, autoriza a conservação de dados pessoais após o término do seu tratamento para o uso exclusivo do controlador, vedado o seu acesso por terceiros e desde que anonimizados os dados. No entanto, considerando os demais e anteriores incisos[5], fato é que a LGPD não condiciona a conservação de dados anonimizados, após o término do tratamento dos dados pessoais, ao cumprimento do princípio da necessidade (artigo 6º, III, LGPD), nem cria quaisquer obrigações aplicáveis aos dados anonimizados. Com efeito, a indicação prevista no parágrafo 39 do Estudo Preliminar parece criar uma obrigação adicional não prevista na legislação de proteção de dados pessoais, ao atribuir uma interpretação mais restritiva do que aquela determinada inicialmente pelo legislador.

Além disso, cumpre ressaltar que os dados anonimizados não estão sujeitos à normativa consagrada pela LGPD, inclusive ao princípio da necessidade, sendo certo que os dados anonimizados não serão considerados dados pessoais (artigo 12, LGPD). Nesse sentido, o controlador pode utilizá-los para a realização de suas finalidades, sem que haja a obrigação de limitar as suas operações ao mínimo necessário para a concretização dos seus propósitos ou de abranger somente dados pertinentes, proporcionais e não excessivos em relação às finalidades iniciais do tratamento dos dados pessoais não anonimizados (artigo 6º, III, LGPD). Em outras palavras, a partir da anonimização das informações, o controlador tem a liberdade de empregá-las a partir de parâmetros próprios para quais finalidades lícitas preferir, sem que a LGPD lhe seja aplicável, de sorte que a ANBC recomenda a exclusão da menção ao princípio da necessidade no parágrafo 39 do Estudo Preliminar.

3. Riscos de reidentificação de dados anonimizados

[5] Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

I - cumprimento de obrigação legal ou regulatória pelo controlador;

II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou

a. Responsabilidade do controlador pela reidentificação do titular

A ANPD sustenta no parágrafo 31 do Estudo Preliminar que a anonimização não seria um processo capaz de transformar em legítima a irregular atividade de tratamento de dados, sem fundamentação legal. À luz dessa afirmação, haveria um risco de responsabilização do controlador pela reidentificação posterior do titular dos dados pessoais conduzida por terceiros, na hipótese de reversão do processo de anonimização.

Assim, a ANBC considera importante a revisão do Estudo Preliminar, de modo que se indique expressamente que eventual reversão do processo de anonimização, levando à reidentificação do titular por terceiros, não configura tratamento irregular de dados pessoais pelo agente que anonimizou as informações. Além disso, não haveria violação de qualquer dispositivo da LGPD por parte do agente, tendo em vista que, segundo a legislação, a reversão do processo de anonimização somente é capaz de responsabilizar o agente quando ocorrer a partir da utilização de meios próprios, na forma do artigo 12 da LGPD. Desse modo, o agente que não realizou o tratamento irregular de dados pessoais (artigo 43, I, LGPD), não pode ser considerado responsável pela reidentificação de titulares realizada por terceiros.

Com isso, a ANPD poderia indicar diretamente em seu Estudo Preliminar, mais especificamente no parágrafo 61, que entenderá pelo não descumprimento da LGPD, e que não aplicará sanções específicas ao controlador, quando o processo de reidentificação do titular for realizado por terceiros, sem que haja culpa do agente que anonimizou os dados. Em outras palavras, caso o controlador adote todas as medidas de segurança e demais requisitos previstos na LGPD, não poderá ser penalizado pela reidentificação realizada por terceiros, tendo em vista que nenhum processo de anonimização é perpétuo (Apêndice I, alínea “c”, do Estudo Preliminar).

Além disso, como a LGPD indica que a anonimização corresponde à utilização de meios técnicos razoáveis e disponíveis no momento do tratamento (artigo 5º, XI, LGPD), a ANPD também poderia esclarecer em seu guia orientativo que, caso novas tecnologias sejam capazes de reverter o processo de anonimização anteriormente conduzido pelo agente de tratamento, este último não poderá ser responsabilizado pela reidentificação possibilitada pelo surgimento dessas novas técnicas. Na mesma linha descrita no ponto anterior, a reidentificação posterior do titular realizada por terceiros a partir de nova tecnologia não

disponível quando da anonimização não deve levar à responsabilização do agente, que teria cumprido com as obrigações dispostas na LGPD no momento da condução da anonimização.

Em outras palavras, a Autoridade pode indicar que a responsabilidade do agente que anonimizou os dados deve se limitar às técnicas disponíveis no momento da anonimização. Assim, os agentes devem estar vinculados à tecnologia disponível em seu tempo, devendo adotar as medidas razoáveis e disponíveis para condução dos processos de anonimização.

A ANBC compreende que uma delimitação específica da Autoridade a esse respeito garantirá maior segurança jurídica aos agentes regulados, além de auxiliá-los na avaliação de seus processos de anonimização sob uma lógica de responsabilização pelas técnicas disponíveis no momento da anonimização, sem possibilidade de penalização por novas tecnologias posteriores que superem os meios técnicos razoáveis e disponíveis naquele cenário inicial.

b. Avaliação de robustez dos processos de anonimização

A ANPD indica no parágrafo 43 do Estudo Preliminar que a adoção de modelos baseados em riscos relacionados à identificabilidade de dados mostra-se pertinente na avaliação da robustez do processo de anonimização, desde que referida avaliação não seja episódica ou pontual, mas iterativa e contínua. Apesar de a ANBC concordar que novos riscos de reidentificação possam advir ao longo do tempo, a partir dos avanços tecnológicos e da quantidade de dados auxiliares que se tornam disponíveis, compreende-se que a Autoridade poderia definir com maior precisão o que entende por “avaliação de robustez dos processos de anonimização” por meios iterativos e contínuos.

A título de exemplo, e como sugestão, a ANBC entende que poderiam ser considerados robustos, e indicados diretamente pela ANPD, os processos de anonimização conduzidos por algoritmos, cuja chave criptográfica não seja de conhecimento público – em outras palavras, cuja chave seja de conhecimento exclusivo do agente de tratamento que realiza tal ação – e de forma que se repute razoavelmente complexo, à luz das medidas técnicas de segurança da informação disponíveis a terceiros, realizar a quebra da criptografia dessa chave. Ademais, a ANPD poderia indicar quais questões deveriam ser consideradas pelo controlador em sua análise de risco. Busca-se, portanto, facilitar a definição de critérios no contexto dos processos de anonimização.

Deve-se considerar 'robustos' os processos de anonimização que tiverem passado por algoritmos cuja chave não seja de conhecimento público, ou seja, cuja chave de anonimização seja de conhecimento exclusivo da empresa que realiza tal ação e com nível de quebra de dificuldade razoável.

O desenvolvimento de raciocínio específico da Autoridade na matéria (conforme parágrafo 43) facilitaria o estabelecimento dos critérios de iteratividade e continuidade aplicáveis no contexto de processos de anonimização delimitados, além de garantir maior segurança jurídica aos agentes de tratamento regulados.

c. Gestão do risco de reidentificação

Ao contrário do indicado no parágrafo 62 do Estudo Preliminar, a ANBC entende que não seria possível ao agente de tratamento conduzir a gestão de risco de reidentificação durante o tratamento de dados pessoais, mas somente após o término do processo de anonimização. Nessa etapa final, efetivamente, seria possível avaliar a eficiência das técnicas utilizadas, a fim de afastar a possibilidade de identificação do titular.

Isso porque, em casos concretos, a gestão de riscos apenas pode ser efetivada quando o processo de anonimização tenha se concluído e as informações deixem de referir-se a uma pessoa natural identificada ou identificável – assim, a avaliação da medida de segurança e a análise de riscos teria relação direta com um processo finalizado passível de ser examinado pelo agente –, razão pela qual sugere-se a revisão do parágrafo 62 do Estudo Preliminar.

d. Risco de reidentificação aceitável

Dentre as etapas do processo de anonimização baseado em riscos, a ANPD indica ao agente de tratamento a determinação do Risco de Reidentificação Aceitável para um certo conjunto de dados, com o objetivo de estipular um limite superior para o risco. Essa definição, que seria estipulada somente pelo próprio agente de tratamento, consoante o parágrafo 65 do Estudo Preliminar, pode colidir com os entendimentos fiscalizatórios posteriores da ANPD. Em outras palavras, o agente de tratamento pode identificar um Risco de Reidentificação Aceitável que seja diferente do analisado futuramente pela Autoridade.

Nesse sentido, a definição do Risco de Reidentificação Aceitável pelo próprio agente de tratamento pode gerar insegurança jurídica em eventuais processos de anonimização, motivo pelo qual a ANBC sugere que a Autoridade indique um rol exemplificativo de quais seriam os parâmetros adequados para que o agente procedesse com a ponderação do Risco de Reidentificação Aceitável nesses cenários.

4. As noções de esforços razoáveis e meios próprios

a. Esforços razoáveis para reversão da anonimização

A ANBC entende que a razoabilidade dos esforços para a reversão do processo de anonimização (artigo 12, LGPD) não seria um conceito jurídico indeterminado, como sustenta a ANPD no parágrafo 48 do Estudo Preliminar, ao indicar que a própria Autoridade, como intérprete e aplicadora da LGPD, deveria preencher, com elementos e critérios pertinentes com o caso concreto, a noção de esforços razoáveis.

A bem da verdade, o artigo 12, § 1º, da LGPD, apresenta exemplos de fatores específicos que devem ser utilizados para a definição dos esforços razoáveis empregados em um determinado caso concreto. Logo, a determinação do que é razoável leva em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios (artigo 12, § 1º, LGPD).

Dessa forma, a ANPD pode auxiliar os agentes de tratamento na identificação e na análise dos fatores descritos no artigo 12, § 1º, da LGPD, desde que a Autoridade esteja adstrita ao que dispõe a legislação – notadamente, a previsão de que a reidentificação do titular tem que ser possível pela utilização exclusiva de meios próprios. Com isso, sugere-se a exclusão da menção à teoria do conceito jurídico indeterminado presente no parágrafo 48 do Estudo Preliminar, a fim de não conferir uma competência não prevista na LGPD à Autoridade.

b. Utilização de meios próprios na anonimização

De acordo com o parágrafo 52 do Estudo Preliminar, a avaliação da possibilidade de reidentificação de dados e a reversão do processo de anonimização deve considerar não apenas o uso de meios próprios do agente de tratamento responsável pela anonimização,

mas também a atuação de outras pessoas ou entidades que, com meios e esforços razoáveis, possam reidentificar os dados anonimizados.

Contudo, a LGPD indica expressamente em seu artigo 12 que os dados anonimizados não serão considerados dados pessoais, salvo quando o processo de anonimização puder ser revertido, utilizando exclusivamente meios próprios. Por isso, não seria possível sustentar que a análise de reidentificação deve levar em conta os meios de terceiros, visto que essa previsão não encontra respaldo na lei. Logo, para que não seja criada uma nova obrigação de avaliação ao agente de tratamento, relativa à possibilidade de reidentificação do titular e de reversão do processo de anonimização por terceiros, recomenda-se a modificação do parágrafo 52 do Estudo Preliminar para excluir a referência a meios de terceiros .

5. Os processos de anonimização e pseudonimização

a. Técnicas de anonimização e pseudonimização

A ANPD identifica a substituição de dados, ofuscação de dados, tokenização e mascaramento de dados como técnicas de pseudonimização de informações, conforme o parágrafo 81 do Estudo Preliminar. Todavia, essas técnicas igualmente podem ser aplicadas para fins de anonimização de dados pessoais, à luz do Guide to Basic Anonymisation, da autoridade de proteção de dados de Singapura,[6] bem como do Anonymization Code of Practice, da autoridade de proteção de dados do Reino Unido.[7]

A depender do Risco de Reidentificação Aceitável, o agente de tratamento pode adotar diferentes técnicas para garantir que o processo de anonimização esteja em conformidade com a LGPD e com as orientações da ANPD. Justamente por isso, a ANBC sugere que o Estudo Preliminar indique diretamente, para além de seu Apêndice II, que as técnicas de pseudonimização também podem ser adotadas para processos de anonimização, à exceção das hipóteses de criptografia típica, sobre as quais a Autoridade já se manifestou no parágrafo 81 do Estudo Preliminar.

b. Metodologia eficaz de pseudonimização

[6] PDPC. “Guide to Basic Anonymisation”. Disponível em:<https://www.pdpc.gov.sg/news-and-events/announcements/2022/03/guide-to-basic-anonymisation-now-available>. Acesso em: 26.02.2024.

[7] ICO. “Anonymization Code of Practice”. Disponível em:<https://ico.org.uk/media/1061/anonymisation-code.pdf>. Acesso em: 26.02.2024.

No âmbito dos parágrafos 83 e 84 do Estudo Preliminar, a ANPD parece referenciar diferentes etapas a serem observadas pelos agentes de tratamento no que se relaciona à condução de processos de pseudonimização. Ao adotar uma linguagem que parece indicar novas obrigações aos agentes regulados, sem qualquer correspondente na LGPD que indique esses deveres adicionais e específicos aos controladores, pode-se criar uma insegurança jurídica indesejável para um documento que visa orientar os agentes a respeito de metodologias eficazes para a pseudonimização.

A Autoridade estabelece, por exemplo, que os controladores devem fornecer treinamentos regulares aos seus colaboradores que realizem o tratamento de dados pessoais – obrigação essa que não se encontra especificamente na LGPD e que poderia ser prejudicial para agentes de tratamento de pequeno porte que não possuem condições de garantir esse tipo de atividade de adequação à legislação de proteção de dados pessoais.

Por isso, a ANBC recomenda que o posterior guia orientativo sobre anonimização e pseudonimização adote uma linguagem mais voltada à recomendação de metodologias a serem implementadas pelos agentes de tratamento regulados, a fim de garantir-lhes maior segurança jurídica, sem que haja a criação ou indicação de obrigações adicionais para a adequação à LGPD.

c. Meios automatizados no processo de anonimização

O Apêndice I, alínea "k", do Estudo Preliminar, indica que a anonimização não deve ser totalmente automatizada, dada a importância do contexto e da avaliação geral do processo de anonimização. Para esse raciocínio, a ANPD parece ter se inspirado em documento da autoridade de proteção de dados da Espanha,[8] tendo em vista que os "10 Misunderstanding Related to Anonymisation" apresentam a mesma orientação em seu item 7 ("anonymisation can be fully automated").

Contudo, o título da alínea "k" ("a anonimização não deve ser totalmente automatizada") parece estar em dissonância com o conteúdo remanescente da alínea ("ferramentas

[8] AEPD. "10 Misunderstanding Related to Anonymisation". Disponível em:<https://www.edps.europa.eu/system/files/2021-04/21-04-27_aepd-edps_anonymisation_en_5.pdf>. Acesso em: 26.02.2024.

automatizadas podem ser usadas durante o processo de anonimização, no entanto, dada a importância do contexto e a avaliação geral do processo, poderá ser necessária a intervenção de um especialista humano") e com a própria LGPD.

Isso porque, ao contrário da experiência europeia na matéria, é perfeitamente possível que o processo de anonimização no Brasil ocorra apenas por meios automatizados e sem a participação ou intervenção de humanos. Essa afirmação alinha-se diretamente ao artigo 5º, III, da LGPD, o qual prevê que um dado será considerado anonimizado à luz da utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

Assim, não se recomenda à Autoridade indicar que a anonimização não possa ser "totalmente automatizada", tendo em vista que a LGPD não proíbe a utilização de sistemas automatizados para o processo de anonimização. Na verdade, a lei autoriza que o agente de tratamento utilize os meios disponíveis para garantir o processo, ainda que esses meios compreendam apenas a utilização de sistemas automatizados, motivo pelo qual sugere-se a modificação do Apêndice I, alínea "k", do Estudo Preliminar.

d. Fiscalização dos processos de anonimização

Ao contrário do recente Guia Orientativo sobre Legítimo Interesse,[9] que apresentou indicação específica de elaboração de teste de balanceamento, o Estudo Preliminar não informa aos agentes regulados como a Autoridade poderá analisar os processos de anonimização e pseudonimização. Dessa forma, recomenda-se maior especificação a esse respeito por parte da ANPD, principalmente a fim de garantir mais segurança jurídica nos projetos de adequação constante à LGPD dos agentes de tratamento.

Após essa especificação, a ANBC entende que poderia ser indicado um prazo para que os agentes de tratamento opinem e dialoguem com a Autoridade acerca de como documentar o processo de anonimização, especialmente tendo em vista eventuais processos administrativos fiscalizatórios da ANPD em face das operações conduzidas pelos agentes de tratamento.

6. Uso compartilhado de dados anonimizados e pseudonimizados

[9] ANPD. "ANPD lança Guia Orientativo sobre Legítimo Interesse". Disponível em:<https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-lanca-guia-orientativo-sobre-legitimo-interesse>. Acesso em: 26.02.2024.

A ANBC compreende que o compartilhamento de dados pseudonimizados, sem os seus identificadores, configura para o destinatário dessas informações a coleta de dados anonimizados, uma vez que o terceiro não seria capaz de identificar o titular das informações. Essa é a mesma conclusão da autoridade de proteção de dados do Reino Unido,[10] segundo a qual as mesmas informações podem ser dados pessoais para um agente de tratamento (dados pseudonimizados), e , ao mesmo tempo, consistirem em dados anonimizados para terceiros, a depender das circunstâncias e do contexto do uso compartilhado.

Diante desse racional, recomenda-se que a ANPD inclua semelhante esclarecimento no posterior guia orientativo sobre anonimização e pseudonimização, especialmente para que o destinatário, isto é, o agente para quem os dados estarão anonimizados, não seja responsabilizado pelos riscos relativos ao processo inicial de pseudonimização.

Ademais, a ANBC entende que o uso compartilhado de dados anonimizados, para ambas as partes que operam as informações, não poderia gerar responsabilização do destinatário pelos riscos relativos ao processo de anonimização previamente realizado a esse compartilhamento – uma vez que não seria o destinatário o agente de tratamento responsável por garantir um processo de anonimização em conformidade com a LGPD. Assim, recomenda-se que a ANPD também preveja esse raciocínio específico em seu guia orientativo, especialmente para garantir maior segurança jurídica aos destinatários dessas informações.

* * *

[10] ICO. "Introduction to Anonymisation". Disponível em:<https://ico.org.uk/media/about-the-ico/consultations/2619862/anonymisation-intro-and-first-chapter.pdf>. Acesso em: 26.02.2024.

Contribuições Petrobras para consulta à sociedade sobre anonimização e pseudonimização para proteção de dados

1) Na definição:

“Entretanto, vários algoritmos criptográficos (simétricos, assimétricos e de hash) podem realizar processamentos unidirecionais. Nesses casos atendem os requisitos da anonimização, desde que os dados cifrados sejam úteis.”

COMENTÁRIO: Entendemos que dos três algoritmos citados, apenas o HASH pode ser considerado unidirecional. Algoritmos de criptografia simétricos e assimétricos são reversíveis, mediante uso da chave criptográfica;

2) No parágrafo:

“Considerando a diversidade de natureza, escopo, contexto e finalidade de cada tratamento realizado pelo agente de tratamento, não é possível definir uma métrica única para a mensuração do risco de reidentificação. Por tal razão, este Guia adota a expressão Métrica Contextual para se referir à métrica utilizada para mensurar o RRM de acordo com a realidade de cada agente de tratamento.”

COMENTÁRIO: Sugerimos que haja menção a critérios objetivos para apoiar a decisão da métrica a ser utilizada (p.e.: Finalidade, compartilhamento com terceiro, quantidade de dados). Quanto menor o grau de anonimização requerido, maior deve ser o RRA;

3) Sugerimos que a ANPD consulte os principais fabricantes de soluções de banco de dados para conhecer e avaliar as funcionalidades de anonimização/pseudonimização existentes no mercado;

4) Sugerimos explicitar no documento final se as orientações emanadas valerão para todas as anonimizações existentes ou somente para aquelas realizadas a partir da publicação do documento final;

5) Sugerimos incluir no documento final que, sendo os dados de fato anonimizados, os mesmos podem ser divulgados ou compartilhados com terceiros;

6) Sugerimos esclarecer as opções para informar ao titular sobre a possibilidade da anonimização, por exemplo por meio de aviso de privacidade;

7) Sugerimos esclarecer quanto aos limites de atuação da ANPD na fiscalização de dados anonimizados e quais medidas podem ser efetivamente determinadas. Não está claro se pode ser determinada a exclusão de dados anonimizados, ainda que deixem de ser considerado dados pessoais, ou se seria uma recomendação de boa prática.

Brasília, 1º de março de 2024

Para: Autoridade Nacional de Proteção de Dados - ANPD

De: Leonardi Advogados

Re: Consulta à Sociedade - Estudo Preliminar - Anonimização e pseudonimização para proteção de dados

Leonardi Advogados ("Leonardi") é um escritório especializado em proteção de dados pessoais, privacidade, direito digital e tecnologia, que faz uso da experiência de mais de vinte e cinco anos com esses temas de seu sócio fundador, Marcel Leonardi.

Marcel é Bacharel, Mestre e Doutor em Direito pela USP e tem pós-doutorado pela Berkeley Law. Foi Diretor de Políticas Públicas no Google de 2011 a 2018, onde colaborou intensamente na elaboração do Marco Civil da Internet e da Lei Geral de Proteção de Dados. Também atuou em questões de políticas públicas nos mais variados assuntos do setor de tecnologia e Internet. Especializado em proteção de dados pessoais e certificado pela IAPP em EU Privacy (CIPP/E) e US Privacy (CIPP/US). Autor dos livros "Responsabilidade Civil dos Provedores de Serviços de Internet", "Tutela e Privacidade na Internet" e "Fundamentos de Direito Digital", Marcel é professor da FGVLaw desde 2005, sócio fundador do Leonardi Advogados e Fundador da Leonardi Legal Learning.

Em razão da vasta experiência do escritório no atendimento a demandas complexas de diversos grandes agentes de tratamento de dados pessoais, a Leonardi Advogados gostaria de contribuir para a consulta à Sociedade da ANPD sobre anonimização e pseudonimização para proteção de dados[1]. Na visão do escritório, há pontos cruciais que merecem especial atenção e devem ser esclarecidos e/ou revistos, de forma a aperfeiçoar futuro guia orientativo a respeito do tema.

[1] Disponível em: https://www.gov.br/participamaisbrasil/consulta-a-sociedade-estudo-preliminar-anonimizacao-e-pseudonimizacao-para-protecao-de-dados

1. Considerando o conteúdo do Estudo Preliminar, apresente suas contribuições sobre o texto.

O estudo preliminar sobre anonimização e pseudonimização para a proteção de dados pessoais revelou-se correto em diversos aspectos que envolvem a matéria. Sob a perspectiva da Leonardi Advogados, o documento elucidou de maneira abrangente a temática e apresentou distinções claras entre conceitos essenciais, esclarecimentos relevantes do ponto de vista jurídico, além de ter apresentado, em formato de anexo, técnicas aplicáveis à anonimização e pseudonimização.

Todavia, em relação à matéria, a Leonardi enfatiza a importância de um detalhamento mais aprofundado pela ANPD sobre alguns pontos em específico, conforme será detalhado ao longo desta contribuição.

Inicialmente, a Leonardi considera pertinente destacar uma observação em relação às definições trazidas ainda no Glossário, em especial, o conceito do que seria considerado um "banco de dados". A minuta apresenta o referido conceito como sendo um "conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico". A definição parece restringir o uso do termo "banco de dados" exclusivamente a repositórios estruturados de dados pessoais, não contemplando a possibilidade de estruturas de conjunto de dados anonimizados. No entendimento deste escritório, é recomendável que a minuta considere a inclusão de um termo que abranja também conjuntos de dados anonimizados para melhor refletir a natureza dessas estruturas, podendo ser utilizadas inclusive - a título de exemplo - as expressões "Banco de Dados Anonimizados" ou "Base de Dados Anonimizados".

Outro aspecto fundamental que a Leonardi considera digno de destaque é a distinção entre pseudonimização e anonimização **no contexto do compartilhamento de informações e base de dados entre agentes de tratamento**. Como muito bem descrito no estudo preliminar, o conceito de pseudonimização consiste na atividade de tratamento de dados temporariamente não-identificados, mas que podem ser reidentificados **pelo mesmo controlador** a qualquer tempo, nos termos do artigo 13, parágrafo 4º da LGPD.

Rafael de Barros | 209 | Conj. 71 | Paraíso | CEP 04003-041 leonardi.adv.br

Ainda, não custa lembrar que a principal diferença entre a pseudonimização e anonimização, é a *reversibilidade*: se é possível reverter o processo, os dados serão considerados pseudonimizados e sujeitos à aplicação da LGPD.

É importante destacar que a capacidade do próprio controlador em realizar a reidentificação implica que os dados são pseudonimizados **apenas em relação a ele (=controlador)**, uma vez que, no contexto do compartilhamento, a verdadeira pseudonimização só é alcançada se o terceiro receptor estiver em posse de qualquer informação do controlador que possibilite a identificação dos dados - o que não é o caso na esmagadora maioria dos cenários em que há esse tipo de compartilhamento.

Em outras palavras, a Leonardi destaca que o ponto central desta discussão reside na compreensão de que, para efeitos práticos, o terceiro envolvido está recebendo dados **anonimizados**, uma vez que não possui o "segredo" da pseudonimização (seja uma função *hash* ou outro método). Assim, uma base de dados que é considerada como **pseudonimizada** pelo controlador será considerada, como regra, **anonimizada** para um terceiro receptor, a menos que o terceiro envolvido seja, de alguma forma, capaz de desfazer a pseudonimização ou reidentificar o dado.

Reforçando essa lógica, ao abordar a pseudonimização de dados, a minuta do guia relaciona algumas técnicas consideradas pela Autoridade como compatíveis com a LGPD, como a substituição de dados, a ofuscação de dados, a tokenização, a cifração, o mascaramento e o *salting*. No entanto, embora tais medidas sejam típicas do emprego da técnica de pseudonimização, é preciso ter em consideração que o resultado gerado pela descaracterização de identidade por meio da aplicação de qualquer delas pode culminar em um conjunto de dados anonimizados para uma organização terceira que não seja capaz de, mediante o emprego de esforços razoáveis e por meios próprios, reidentificar os titulares ou restabelecer os dados em sua versão original. Dessa forma, entende-se que as técnicas relacionadas pela Autoridade não representam necessariamente técnicas exclusivas de pseudonimização de dados, podendo também funcionar como técnicas para anonimização de dados em relação a terceiros.

Em síntese, dados considerados **pseudonimizados** da perspectiva da empresa "A" serão, como regra, considerados **anonimizados** da perspectiva da empresa "B" que os recebeu da empresa "A", justamente porque a empresa "B" não dispõe de meios para decifrar o "segredo" da pseudonimização empregada pela empresa "A".

No entendimento da Leonardi, a menção expressa desta distinção no estudo preliminar é essencial para uma compreensão precisa dos conceitos de anonimização e pseudonimização e, inclusive, sob a perspectiva da aplicação prática da LGPD ao longo da cadeia de tratamento, uma vez que dados anonimizados não são considerados dados pessoais e, consequentemente, não se sujeitam à sua aplicação.

No tocante ao que constitui um esforço razoável para a reversibilidade de um processo de anonimização, na visão da Leonardi, o estudo preliminar foi correto ao destacar a importância de levar em consideração a **licitude dos meios utilizados**, descrevendo, inclusive, que crimes cibernéticos ou uso de meios proibidos configuram **esforços irrazoáveis** para esta interpretação.

É possível que o surgimento de novas tecnologias ou a disponibilização futura de novos conjuntos de dados venham a contribuir para a elevação do risco de reversão de processos de anonimização. No entanto, essa possibilidade não deve ser levada em consideração a partir de **situações meramente hipotéticas, irreais ou de difícil ocorrência.**

Além disso, acredita-se que a constatação do surgimento de novas tecnologias capazes de fragilizar ou desconstituir um processo de anonimização de dados não deva gerar efeitos retroativos sobre o uso dos dados anonimizados, de maneira que todas as atividades realizadas em momento anterior à descoberta de tal tecnologia seja reputada como legítima e indene de incidência da legislação de proteção de dados.

Em que pese essas constatações, a Leonardi entende que uma interpretação detalhada sobre os termos "meios próprios" e "esforços razoáveis" deve fazer parte do futuro guia. A interpretação do conceito de "meios próprios" proposta preliminarmente pela Autoridade parece deixar, equivocadamente, de reconhecer a possibilidade de um mesmo conjunto de dados possuir naturezas diferentes para organizações distintas.

Essa interpretação, inclusive, independe do fato de organizações A e B serem, ou não, pertencentes a um mesmo grupo econômico. Tal entendimento está alinhado ao posicionamento do Information Commissioner Office (ICO), no documento *"Introduction to Anonymisation - Draft anonymisation, pseudonymisation and privacy enhancing technologies guidance"*, referência global no tema anonimização de dados.

A Leonardi reforça outro ponto relevante que merece melhor aprofundamento, no que se refere à correlação realizada no documento entre o princípio da finalidade, previsto no Artigo 6, I, LGPD, e a anonimização de dados pessoais. Segundo o estudo preliminar, para que a anonimização esteja em conformidade com a LGPD, o controlador deve informar com clareza, ao coletar um dado pessoal, que uma das finalidades relativas ao tratamento é a futura anonimização dos dados pessoais.

Este escritório, entretanto, entende que não haveria necessidade de fornecer este tipo de informação ao titular - ao menos como descrita no estudo preliminar - sobre a possibilidade de que um dado pessoal venha a ser, futuramente, anonimizado pelo controlador. Uma das razões para este entendimento reside no fato de que os dados anonimizados não são considerados dados pessoais e, portanto, não se sujeitam à aplicação da LGPD.

Em outras palavras, sobre o conjunto de dados tornados anonimizados, não há que se falar em aplicação de quaisquer dos princípios previstos na LGPD. Nesse sentido, não se revela razoável - nem necessário - comunicar ao titular que todo e qualquer tratamento de dados pessoais realizado poderá vir a ser eventualmente anonimizado pelo controlador.

Além disso, a importância em assegurar a transparência ao titular sobre a anonimização de dados pessoais está centrada na ideia de permitir que este questione o controlador em situações nas quais a anonimização apresente problemas. Logo, a comunicação de forma ampla e antecipada ao titular sobre eventual anonimização dos dados mostra-se dispensável, tendo em vista que o controlador poderá decidir, inclusive, pela eliminação destes ao invés de realizar o processo de anonimização, conforme sua própria conveniência.

Sobre a anonimização de dados, a minuta apresentada propõe que a avaliação da compatibilidade da anonimização de dados leve em consideração "o contexto da atividade de tratamento de dados pessoais, **os riscos envolvidos** e outras circunstâncias relevantes do caso concreto". No entanto, é crucial que o documento esclareça quais seriam, na perspectiva da Autoridade, os riscos a serem efetivamente considerados na referida avaliação. Isso implica definir se seriam riscos associados à atividade de tratamento de dados pessoais pelo controlador originário, riscos inerentes ao processo de anonimização dos dados, riscos decorrentes do uso dos dados anonimizados ou relacionados à possibilidade de reversão da anonimização.

Mais adiante, a minuta de Guia Orientativo afirma que o processo de anonimização recai sobre os elementos identificadores (diretos ou indiretos) de um conjunto de dados, o que, acredita-se, esteja correto. Sob a perspectiva da Leonardi, seria importante, porém, deixar expressa a possibilidade de o processo de anonimização ser considerado eficaz ainda que identificadores indiretos não sejam completamente removidos, prejudicados ou tornados inúteis dentro de um conjunto de dados, sempre que a probabilidade de reidentificação dos titulares permaneça em nível suficientemente remoto. Por exemplo, certos identificadores indiretos, como gênero, estado e idade, normalmente podem ser utilizados dentro de um conjunto de dados anonimizados sem que haja possibilidade de identificação de seus titulares.

Nessa mesma ordem de ideias, o estudo preliminar afirma que a avaliação de compatibilidade da anonimização de dados leve em consideração *"as expectativas legítimas dos titulares e os possíveis impactos do tratamento posterior sobre seus direitos"*. Porém, a consideração das expectativas legítimas dos titulares é tema relacionado ao uso do legítimo interesse como base legal de tratamento. A LGPD não impõe que "expectativas legítimas" dos titulares sejam consideradas como um fator relevante para legitimar o processo de anonimização de dados, inclusive porque o processo de anonimização pode ser complexo e pouco compreensível à pessoa média, sendo irrazoável pressupor que alguém, sem razão aparente, teria uma efetiva expectativa de que seus dados pudessem ser submetidos a um processo de anonimização em determinado momento ou contexto.

Outro ponto relevante se refere à ideia de que *"a pertinência da adoção do processo de anonimização decorre de um juízo de necessidade"* pelo agente de tratamento, que seria realizado *"à luz da(s) finalidade(s) especificada(s) para o tratamento de dados na situação concreta"*. No entanto, a aplicação do processo de anonimização não decorre, exclusivamente, de uma necessidade constatada, podendo derivar de uma conveniência ou oportunidade identificada pelo agente. A anonimização de dados pode ser tida como uma medida relevante para a realização de atividades econômicas de maneira mais compatível com a segurança e com a privacidade, ainda que existam alternativas que permitam ao agente alcançar as mesmas finalidades sem anonimizar os dados. Nesse caso, o agente de tratamento decide a respeito da anonimização de dados à luz de um juízo de relevância e conveniência, e não de mera necessidade. Dessa forma, é prudente que o futuro guia sobre o tema mencione, de forma expressa, que a anonimização pode decorrer de necessidade, relevância ou conveniência.

Por fim, quanto às técnicas de anonimização mencionadas pela ANPD, esta sugere que a aplicação da função hash funcionaria exclusivamente como uma ferramenta de pseudonimização - o que também não é entendido como correto por este escritório. A substituição por códigos hash pode, em inúmeras situações, resultar numa massa de dados pseudonimizados para uma determinada organização e a mesma massa de dados resultar em dados anonimizados para outra organização. Isto é, uma mesma massa de dados gerados após a aplicação da técnica por hash pode ser utilizada por mais de uma organização, mas que apenas uma dessas organizações possua o valor de entrada capaz de reverter o código hash.

Sobre o processo de pseudonimização, a minuta reforça a necessidade de uma análise cuidadosa da expressão "mantidas separadamente". Todavia, este escritório entende ser essencial que o Guia Orientativo forneça orientações mais detalhadas sobre como os agentes de tratamento devem interpretar essa expressão, esclarecendo se os "segredos de pseudonimização" devem ser mantidos em bancos de dados distintos e dedicados - completamente segregados dos bancos de dados que armazenam os dados pseudonimizados - ou se a convivência de tais informações em um mesmo banco de dados - mas em repositórios distintos de um mesmo suporte eletrônico ou físico - seria suficiente para atender à exigência normativa.

A minuta também apresenta fluxo para pseudonimização ("Metodologia Eficaz de Pseudonimização") com 12 etapas - entre as quais a elaboração de uma avaliação de impacto à proteção de dados pessoais (etapa 11). No entanto, esse ponto merece ser melhor esclarecido, para que não se crie nos agentes de tratamento uma falsa percepção de que todas as atividades envolvendo pseudonimização de dados demandariam a condução de um Relatório de Impacto à Proteção de Dados Pessoais de maneira indiscriminada, posto que a atividade de pseudonimização, por si só, é incapaz de gerar alto risco às liberdades e aos direitos dos titulares (requisito essencial para a necessidade de elaboração de um RIPD). Referido posicionamento, de maneira mais objetiva, evitará que os agentes de tratamento sofram com ônus operacionais e financeiros na condução de RIPDs desnecessários.

Entre as etapas inseridas na "Metodologia Eficaz de Pseudonimização", está a comunicação aos titulares. A minuta sugere que o agente de tratamento deve estar *"preparado para informar de forma transparente e acessível aos titulares sobre a pseudonimização"*. No entanto, a LGPD não prevê a comunicação com os titulares como um pressuposto essencial à aplicação das técnicas de pseudonimização de dados. O dever de comunicação com os titulares (princípio da transparência) deve ser regularmente aplicado a todas as atividades de tratamento que envolvam dados pessoais, sem qualquer tipo de obrigação incremental nas atividades envolvendo a pseudonimização de dados. Caso mantido esse entendimento, a Leonardi sugere que sejam apresentadas diretrizes concretas sobre o contexto no qual essa comunicação se mostraria exigível, bem como seu conteúdo e escopo esperados. Acredita-se que questões pura ou majoritariamente técnicas, como a modalidade de pseudonimização aplicada pelo agente de tratamento, não devam ser reveladas, sob pena de potencialização dos riscos de tentativas externas de reversão da técnica empregada.

Outra etapa inserida na referida metodologia apresentada consiste no treinamento e conscientização de pessoas. Ao abordar o tema, o material sugere que os agentes de tratamento forneçam treinamentos aos seus times internos para que *"compreendam a importância da pseudonimização e* ***saibam como aplicá-lo corretamente***". A redação parece sugerir que qualquer colaborador da organização possa aplicar técnicas de pseudonimização durante o uso de dados pessoais.

No entanto, ao contrário disso, entende-se que a Autoridade melhor atuaria esclarecendo que os processos de pseudonimização devem ser aplicados pelas áreas técnicas responsáveis na organização, como os departamentos de tecnologia, privacidade, segurança da informação, data analytics, ou áreas equivalentes que disponham de conhecimento e capacidade suficientes para garantir a segurança do processo. Este registro pela Autoridade, de maneira expressa, reduzirá oportunidades para que o processo de pseudonimização de dados, na prática, seja deixado a cargo de áreas desprovidas de conhecimento e capacidade técnica suficientes.

Sobre técnicas de criptografia, o Guia disponibilizado prevê objetivamente que "criptografia típica não é anonimização". Do ponto de vista deste escritório, entendimento absoluto como este tende a não ser a melhor solução para o tema. Argumentamos. A aplicação de técnicas de criptografia é capaz de gerar uma massa ou uma base de dados pseudonimizados - especialmente em contextos específicos - para uma determinada organização e, para outra organização, uma base ou massa de dados anonimizados. É possível que essa massa de dados gerados após a aplicação da técnica de criptografia seja utilizada por mais de uma organização, mas que apenas uma dessas organizações possua a chave reversível de desencriptação - independentemente de tais organizações serem ou não de um mesmo grupo econômico.

Mais adiante, a minuta inaugura dois conceitos sobre a gestão de riscos vinculada à anonimização de dados pessoais: Risco de Reidentificação Aceitável (RRA) e Risco de Reidentificação Mensurado (RRM). De acordo com o entendimento sugerido, os agentes de tratamento deveriam estabelecer um Risco de Reidentificação Aceitável (RRA) e contra esse RRA compararem, casuisticamente, os Riscos de Reidentificação Mensurados (RRM) apurados em casos concretos de anonimização. A partir disso, nos casos em que o RRM superasse o RRA o processo de anonimização não se reputaria efetivo ou satisfatório. No entanto, entende-se que, ao contrário do entendimento trazido pela Autoridade, eventual apuração de um RRM em patamar superior ao RRA estabelecido previamente pelo agente não deve, por si só, descaracterizar a natureza do conjunto de dados como anonimizados, pois a probabilidade de reidentificação pode ser suficientemente remota ainda que excedente ao apetite ao risco do agente de tratamento (definido no RRA). Nesse caso, sob a perspectiva da Leonardi, o agente deveria apenas adotar medidas adicionais para que o processo de anonimização apresentasse um RRM compatível e inferior ao RRA.

Sobre este tema, a minuta também afirma que os seguintes elementos devem ser levados em consideração durante a **avaliação dos riscos de reidentificação** sobre dados anonimizados: a distinção (singling-out), a possibilidade de ligação (linkability) e a inferência (inference). Ainda que tal posicionamento esteja alinhado à interpretação europeia sobre o tema (inclusive com referências expressas do Information Commissioner Office), a Leonardi pondera que a mera associação de dados a respeito de um mesmo indivíduo desconhecido, ou a extração de presunções sobre grupos de pessoas não identificadas ou identificáveis, é incapaz de prejudicar ou tornar ineficaz o processo de anonimização de dados. Em caso de entendimento diverso por parte da Autoridade, o uso de dados anonimizados se mostraria substancialmente inútil em boa parte dos casos de uso mais relevantes ao tema, tornando, eventualmente, a regulação totalmente avessa à realidade.

Para concluir, a Leonardi enfatiza o trecho trazido no estudo preliminar, o qual ressalta que dados pessoais submetidos ao processo de anonimização devem ser, na origem, objeto de legítimo tratamento pelo agente responsável. O estudo esclarece que o processo de anonimização não tem a capacidade de legitimar atividades de tratamento originalmente ilícitas - com o que concordamos - porém, não menciona a ausência de responsabilidade do agente de tratamento que recebe dados pessoais já anonimizados, tendo em vista que não participou do processo da coleta desses dados em sua origem e, consequentemente, não possui qualquer informação sobre a sua forma de obtenção.

Este é um ponto que merece constar da versão final do documento: **a ausência de responsabilidade do terceiro receptor que recebe dados anonimizados de outro agente de tratamento.** Isso se justifica em razão de duas ideias centrais: em primeiro lugar, o terceiro não dispõe de meios para verificar se o dado recebido foi obtido de maneira lícita ou ilícita na origem; em segundo lugar, o dado recebido, uma vez anonimizado, não está sujeito à aplicação da LGPD.

Estes são os principais tópicos que a Leonardi Advogados entende que merecem ser abordados com maiores detalhes na versão final do material produzido pela ANPD, de forma a trazer clareza e segurança jurídica aos agentes de tratamento.

Zetta

Contribuições da ZETTA ao Estudo Preliminar da ANPD sobre a minuta do Guia de Anonimização e Pseudonimização para a Proteção de Dados Pessoais

São Paulo, 14 de março de 2024.

A Zetta, associação sem fins lucrativos que representa empresas de tecnologia constituídas como plataformas de serviços financeiros digitais, vem, por meio desta manifestação, apresentar contribuições para a Consulta aberta pela Autoridade Nacional de Proteção de Dados (“ANPD”) à Sociedade sobre a minuta do Guia de Anonimização e Pseudonimização para a Proteção de Dados Pessoais, publicada em 30 de janeiro de 2024 juntamente a um estudo preliminar elaborado pela ANPD sobre o tema ("Estudo Preliminar").

Em virtude do impacto que as futuras orientações e regulamentações da ANPD sobre anonimização e pseudonimização podem trazer para a continuidade e o futuro do modelo de negócio de suas empresas e até mesmo para o Sistema Financeiro Nacional, a Zetta apresenta abaixo as suas contribuições.

Conceitos básicos

O item 2 do Estudo Técnico introduz, no seu subitem 2.1, um glossário no qual são apresentadas definições relacionadas ao tema da anonimização e da pseudonimização. Algumas dessas definições, como "identificador direto" e "identificador indireto", são bastante relevantes, mas não estão presentes na LGPD. Diante disso, nossa sugestão seria remover essas definições do Estudo Preliminar e inseri-las no Glossário de Proteção de Dados Pessoais e Privacidade publicado pela ANPD em 31/01/2024, ao qual o Estudo Técnico faria referência. O objetivo é centralizar as definições relacionadas ao arcabouço regulatório de proteção de dados do país em um único documento, possibilitando a aplicação das definições do Estudo Preliminar em outros contextos, padronizando os conceitos utilizados, e assegurando maior segurança jurídica aos agentes de tratamento de dados pessoais e aos titulares.

Ainda em relação ao subitem 2.1, seria importante haver maior esclarecimento sobre a definição de "Dado em fluxo" (definido pelo Estudo Técnico como "Dado gerado continuamente a uma alta taxa de velocidade, com tamanho potencialmente infinito e necessidade de processamento imediato"), particularmente em relação ao que a ANPD interpreta como "tamanho potencialmente infinito" de um dado.

Informação ao titular sobre a anonimização

Os itens 32 a 40 do Estudo Preliminar visam obrigar o controlador a informar o titular dos dados sobre a finalidade da anonimização dos dados desde o início do tratamento, dado que a operação de anonimização constitui uma forma de tratamento. Caso contrário, o controlador estaria obrigado a utilizar os dados de

maneira compatível com a finalidade inicialmente informada ao titular de dados pessoais.

Tal medida, caso implementada, é capaz de afastar o uso do instituto da anonimização de dados pelo controlador. Isso porque o controlador enfrentaria não apenas a necessidade de remover identificadores, mas também a restrição quanto ao escopo e propósito do uso desses dados.

Em última análise, tais medidas podem impactar significativamente a forma como os controladores lidam com a anonimização de dados e suas práticas de tratamento de dados pessoais. Na prática, é muito comum que empresas lidando com uma ampla base de clientes tenham que utilizar-se de estatísticas sobre o comportamento e preferências da base para otimizar seus produtos e serviços de acordo com os padrões de mercado. A anonimização prevista na LGPD faculta às empresas uma forma de proteção da privacidade e dos dados pessoais de seus titulares, sem comprometimento do uso de dados em legítimo interesse e de acordo com finalidades particulares de cada empresa (que podem, inclusive, fazer parte de seus segredos comerciais).

Considerando o baixo risco de reidentificação, a anonimização feita corretamente e segundo os melhores meios técnicos disponíveis assegura ao controlador a liberdade para tratar os dados conforme finalidades diversas, a seu critério, dado que não mais seriam dados pessoais nem estariam cobertos pelas obrigações da LGPD. Por essa razão, a obrigação de informar os titulares de dados sobre futuras intenções de anonimização ou restrição de finalidades para o tratamento impõe limitações significativas ao controlador, dificultando qualquer abordagem original, criativa ou inesperada no momento da coleta de dados.

Além disso, não há qualquer comprovação de que comunicar os titulares acerca da anonimização dos seus dados lhes traga benefícios efetivos, para além da transparência que já possuem ao saber que os dados serão tratados mediante bases legais adequadas.

Diante do exposto, entendemos que, como a anonimização deverá contar com uma base legal válida para que possa ser feita de maneira legítima, não haveria necessidade de informar os titulares a respeito da prática de anonimização dos seus dados.

Riscos de reidentificação

Ao tratar de “riscos de reidentificação” no item 44, o Estudo Preliminar menciona que “uma avaliação de risco envolve a catalogação da variedade de potenciais atacantes, e, para cada um, a probabilidade de sucesso”, e alega que a figura de um hipotético “atacante” possui certas habilidades, conhecimento ou acesso. Entretanto, a indefinição de critérios objetivos sobre quais seriam estas “habilidades, conhecimento ou (nível de) acesso” de um “atacante” torna problemática a mensuração dos riscos de reidentificação. Por essa razão, sugerimos a definição de critérios mínimos para auxiliar na avaliação de riscos de reidentificação.

Esforços razoáveis

O item 48 do Estudo Preliminar determina que a ANPD deve preencher, com elementos e critérios pertinentes com o caso concreto, a noção de “esforços razoáveis”. Entendemos que a interpretação do que seria "esforços razoáveis", além de conceder subjetividade considerável na aplicação da legislação, aumenta o ônus da Autoridade quanto a essa interpretação, razão pela qual acreditamos que o detalhamento dessa definição se mostra necessário.

Meios próprios

Já o item 52 do Estudo Técnico, ao tratar de "meios próprios", determina que a avaliação da possibilidade de reidentificação de dados e a reversão do processo de anonimização devem levar em consideração não apenas o uso de meios próprios do agente de tratamento responsável pela anonimização, mas também a atuação de outras pessoas ou entidades que, com meios e esforços razoáveis, podem reidentificar conjunto de dados anonimizados. Ocorre que o processo de anonimização muitas vezes conta com o apoio de ferramentas de terceiros (ainda que licenciadas pelo agente), de modo que o emprego do conceito de "meios próprios" pode fomentar a redução do uso de certas técnicas de anonimização que são inclusive reconhecidas pelo mercado. Considerando o exposto, acreditamos que seria interessante reformular esse item, a fim de oferecer maior segurança jurídica quanto à sua interpretação.

Análise sobre o grau de anonimização

Nos itens 58 e 59 do Estudo Técnico, a ANPD discorre sobre o fato de que uma atividade de tratamento de dados pessoais deve estar atrelada a uma finalidade específica, cabendo ao agente de tratamento identificar o grau de utilidade do dado pessoal para alcançar a finalidade especificada, e, consequentemente, estabelecer o grau necessário de anonimização dos dados. No nosso entendimento, essa análise, além de onerosa para os agentes de tratamento, mostra-se arbitrária, haja vista que os princípios de tratamento de dados pessoais (como necessidade e minimização), quando devidamente observados, afastam a obrigatoriedade de anonimização dos dados pessoais. Logo, entendemos que a anonimização de determinados dados pessoais deveria ser uma escolha do agente de tratamento de acordo com as peculiaridades do caso concreto, e não uma imposição regulatória.

Continuidade da gestão do risco de reidentificação

O item 62 menciona que a gestão do risco de reidentificação deve ser realizada de forma contínua durante todo o tratamento dos dados, permitindo que o agente de tratamento tenha evidências suficientes para a tomada de decisão relacionada à proteção de dados e à privacidade dos titulares. Para isso, a ANPD lista várias etapas que devem ser seguidas nesse processo de risco. Ocorre que essa gestão de risco contínua pode ser demasiadamente onerosa para o agente de tratamento, que deveria ser o responsável pela decisão de quais técnicas de avaliação de risco serão adotadas. Logo, acreditamos que as etapas apresentadas no

Estudo Técnico devem ser meramente sugestivas ou exemplificativas, e não obrigatórias.

Métrica de risco de reidentificação

No item 72 do Estudo, consta que a métrica de risco de reidentificação pode ser computada para cada um dos titulares pertencentes ao conjunto de dados, e os valores resultantes podem ser ponderados, por exemplo, com a média aritmética, para determinar o valor geral da métrica contextual. Nesse ponto, seria interessante que a ANPD esclarecesse se essa métrica valeria para cada um dos titulares individualmente (o que poderia gerar uma onerosidade excessiva ao agente de tratamento), ou para cada categoria de titular, a fim de oferecer maior segurança jurídica quanto à sua interpretação.

Metodologia Eficaz de Pseudonimização

No que concerne à Metodologia Eficaz de Pseudonimização, indicada no item 83 do Estudo Técnico, constata-se que o cumprimento de todas as suas etapas é excessivamente burocrático, especialmente considerando que muitos dos seus requisitos já são cumpridos pelos agentes de tratamento em decorrência da própria observância da LGPD (e.g., governança interna de proteção de dados). Além disso, também questionamos a real necessidade de comunicar os titulares de dados acerca da pseudonimização dos seus dados, considerando que a pseudonomização não implica em nenhuma finalidade adicional de tratamento desses dados, e de elaborar um RIPD para os fluxos de pseudonimização, como se todos fossem tratamentos que trazem riscos altos ou muito altos aos titulares.

Ainda, consideramos que as etapas propostas pelo Estudo Técnico devem ser meramente exemplificativas, ficando à critério das organizações a melhor forma de desenvolver, aplicar e documentar processos de pseudonimização, a fim de evitar a imposição de encargos adicionais aos agentes de tratamento.

Zetta

SOBRE A ZETTA

A ZETTA é uma associação sem fins lucrativos que reúne empresas de tecnologia que oferecem serviços financeiros digitais. Nosso objetivo é garantir um ambiente econômico competitivo que resulte em maior inclusão financeira, inovação e satisfação dos clientes. A Zetta tem por missão dar visibilidade aos posicionamentos e ideias do setor aos reguladores, parlamentares e outros atores envolvidos no processo de formulação, implementação e avaliação de políticas públicas. Atualmente, são associados da Zetta as seguintes empresas de tecnologia: **99 Pay, Agibank, Banco VR, Bitso, Caju, Cappta, CERC, Cloudwalk, Cora, CSU Digital, Fitbank, Fintech Magalu, IFood, Isaac, Iugu, Mercado Pago, NaturaPay, Neon, Nubank, PicPay, Recarga Pay, Transfero, Unico, WillBank, Wise, Z1 e Zoop.**

Contribuição à Consulta Pública ANPD sobre Anonimização

DANIEL

São Paulo, 14 de março de 2024.

À AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS
Via e-mail:

DANIEL ADVOGADOS vem, respeitosamente, apresentar suas contribuições no âmbito da Consulta Pública sobre Anonimização.

Cumpre ressalvar que este escritório também manifestou suas considerações via "Participa + Brasil", mas, em razão da extensão dos apontamentos e limitação de caracteres da plataforma, entendeu por bem encaminhar a íntegra por meio da presente comunicação.

Por fim, este escritório aproveita para congratular a abertura da Autoridade às Consultas Públicas e renovar seus votos de estima e consideração.

DANIEL ADVOGADOS

	Tema	Item do Estudo Preliminar	Contribuição
I	**Aplicabilidade dos princípios e deveres da LGPD ao processo de anonimização**	Item 3.1.1, parágrafo 37	Explicitar que a avaliação da compatibilidade da anonimização com as finalidades originárias do tratamento refere-se exclusivamente ao momento anterior ao processo de anonimização, quando há tratamento de dados pessoais. Uma vez que, após a anonimização, os dados não são mais considerados pessoais e, consequentemente, não estão mais sob o âmbito de incidência da LGPD e de seus princípios.
II	**Risco de reidentificação**	Item 3.1.2	Importante incluir exemplos de técnicas de anonimização em práticas comuns de mercado, como em casos de dados não estruturados e em uso de inteligência artificial, para melhor orientação a seguir.
III	**Noções de esforços razoáveis e meios próprios**	Item 3.1.3	Considerar a diferença entre o conteúdo da *Consideranda* 29 do GDPR, que não menciona “meios próprios” e o artigo 12, LGPD que o faz, ao estabelecer o que deve ser considerado na delimitação de reidentificação dos dados pessoais anonimizados. A possibilidade de reidentificação no Brasil deve ser, "exclusivamente por meios próprios”.
IV	**Gestão do risco de reidentificação**	Item 3.2.2	Considerar o procedimento em etapas indicado como “Gestão do risco de reidentificação” como uma boa prática recomendada pela Autoridade, mas não um requerimento legal para a anomização, haja vista que não constituir “padrão ou técnica utilizada em processo de anonimização”, nos termos do art. 12, §3º, LGPD.

I. APLICABILIDADE DOS PRINCÍPIOS E DEVERES DA LGPD AO PROCESSO DE ANONIMIZAÇÃO (item 3.1.1.)

No item 3.1.1. do Estudo Preliminar, a Autoridade sustenta que a anonimização é um processo por meio do qual serão aplicadas variadas técnicas de modo a desassociar os identificadores diretos e indiretos do dado do seu estado originário. De acordo com a autoridade, os dados pessoais objeto do processo de anonimização devem originalmente ter sido tratados de forma lícita e legítima, justificados por uma base legal e aderentes aos princípios da finalidade, adequação e necessidade.

Com o intuito de melhor elucidar o tópico, a Autoridade, no parágrafo 37 do estudo, indica como técnica de avaliação da compatibilidade da anonimização com as finalidades originárias do tratamento, a avalição descrita no Guia Orientativo – Tratamento de Dados Pessoais Pelo Poder Público, a qual prevê que o agente de tratamento deve avaliar:

(i) contexto da atividade, riscos envolvidos e outras circunstâncias relevantes para o tratamento;

(ii) a conexão fática e jurídica entre a finalidade originária e os objetivos do processo de anonimização; e

(iii) a expectativa do titular dos dados e os impactos do tratamento posterior em relação aos seus direitos.

Contudo, seria importante explicitar que a referida avaliação somente seria aplicável antes do processo de anonimização, uma vez que este bem-sucedido, não mais os dados tratados estariam sob o âmbito de incidência da LGPD pois não seriam pessoais, nos termos definidos no art. 5, inciso I e II e do art. 12.

O momento do ciclo de vida do dado, se antes ou depois do processo de anonimização importa, haja vista que após esse processo não mais se pode falar em dado pessoal e, consequentemente, de aplicabilidade da LGPD. Assim, os usos dos dados após o processo de anonimização não estão sob a égide da LGPD e não precisam ser lastreados nos princípios da finalidade, adequação e necessidade que originalmente balizaram o tratamento, e pelos mesmos motivos, tampouco há necessidade de correspondência entre

esses usos e aqueles que motivaram inicialmente o tratamento dos dados pessoais.

É importante que o texto do estudo traga maior clareza quanto ao ponto de modo a não gerar dúvidas quanto aos limites do uso de dados anonimizados e quanto a obrigatoriedade de utilização do procedimento indicado.

II. RISCO DE REIDENTIFICAÇÃO (item 3.1.2.)

No item 3.1.2., a Autoridade sustenta que o processo de anonimização admite abordagens e metodologias diversificadas, cuja pertinência seria justificada pelas características e os aspectos contextuais do banco de dados que o agente de tratamento pretende anonimizar, fazendo referência aos Apêndices II e III de exemplos de técnicas de anonimização para tal.

Contudo, é importante que os casos apresentados nos Apêndices sejam diversificados em relação a práticas de mercado, que comumente incluem dados não estruturados e utilização de inteligência artificial, de forma a orientar sobre o caminho mais adequado a se seguir na realização do processo de anonimização.

III. NOÇÕES DE ESFORÇOS RAZOÁVEIS E MEIOS PRÓPRIOS (item 3.1.3)

No item 3.1.3. do estudo, a Autoridade elucida que o entendimento do processo de anonimização e dos critérios a serem considerados para avaliar o risco de reidentificação dependem da compreensão dos conceitos de "esforços razoáveis" e "meios próprios" descritos no art.12 da LGPD.

No primeiro caso, aponta a Autoridade, que a noção de "esforço razoável" é um conceito jurídico indeterminado que deveria ser preenchido valorativamente pelo aplicador do Direito, inclusive pela própria autoridade, com base no rol exemplificativo de conteúdo objetivo do art.12 §1º da LGPD, o qual apresenta fatores como: custo e tempo para reverter o processo de anonimização, a existência

de tecnologias e técnicas disponíveis ao tempo da operação capazes de reverter a anonimização, bem como, a licitude dos meios utilizados para efetivar o processo de anonimização.

Essa interpretação já é bastante conhecida, não só por estar prevista na lei, como também por ser baseada exclusivamente em decisões do Tribunal de Justiça da União Europeia e em pareceres e interpretações do extinto Grupo de Trabalho do Artigo 29 da União Europeia.

Nesse contexto, e considerando a disciplina de anonimização de dados adotada na LGPD que atrela o uso exclusivo de meios próprios ao emprego dos esforços razoáveis para efetivar o processo de anonimização, seria importante que a Autoridade trouxesse maior concretude sobre a interpretação do que pode ser considerado no conceito de "esforços razoáveis".

No segundo caso, aponta a Autoridade que o significado da expressão meios próprios se refere ao uso de habilidades, técnicas, instrumentos e tecnologias disponíveis pelos próprio agente responsável pela anonimização.

No entanto, ao retomar o ponto da possibilidade de reidentificação de dados e reversão do processo de anonimização, a Autoridade reforça o posicionamento de abordagem objetiva adotada pela União Europeia, isto é, que o agente deve considerar na análise de risco de reidentificação não somente os seus próprios esforços, como também a autuação de outras pessoas e entidades, as quais, com esforços razoáveis, poderiam reindentificar os dados.

Da análise do "Estudo Técnico sobre a anonimização de dados na LGPD: análise jurídica" é possível compreender que o ponto foi deduzido pela aparente aproximação do conteúdo da Consideranda n.29 do GDPR com aquele descrito no art.12 da LGPD. Ocorre que o GDPR ao tratar de anonimização não cita a possibilidade de utilização exclusiva de meios próprios, tal como a LGPD o faz, tampouco, atribui ao texto da Consideranda força normativa, apenas,

orientativa aos agentes de tratamento que atuam no bloco europeu.

Assim, é importante que a Autoridade esclareça o ponto sobre a necessidade de análise dos risco de reidentificação englobar ou não esforços de terceiros, haja vista que o art. 12 da LGPD trata exclusivamente de meios próprios. Caso esta entenda, que, de fato, o modelo brasileiro se aproxima ao modelo objetivo europeu, faz-se necessário que haja maiores explicações frente a opção legislativa do art. 12, de restringir-se aos "meios próprios".

IV. GESTÃO DO RISCO DE REIDENTIFICAÇÃO (3.2.2.)

No item 3.2.2. do estudo, a Autoridade propõe um processo de anonimização baseado em risco dividido em 04 etapas, quais sejam:

(i) determinação do Risco de Reidentificação Aceitável (RRA), cujo objetivo é definir o limite superior para o risco;

(ii) aplicação do conjunto de técnicas de anonimização escolhido, cujo objetivo é produzir um conjunto de dados anonimizados com risco de reidentificação inferior ao limite de risco aceitável;

(iii) definição de um Risco de Reidentificação Mensurado (RRM), probabilidade de um ataque de reidentificação ser bem-sucedido com base na métrica contextual;

(iv) comparar o RRA ao RRM de modo a identificar se os dados apresentam condição de estarem anonimizados.

Em relação ao tópico, sugerimos que seja adotada uma noção ampla da análise de risco de reindendificação de modo que o processo citado seja apenas uma das diferentes possibilidades existentes em que o agente de tratamento pode se utilizar para verificar o grau de risco da anonimização em determinado processo, como é o caso das análises contextuais.

Isso porque ao não se tratar, tecnicamente, de padrão ou técnica de anonimização, e sim de análise de risco, extrapola o âmbito de competência estabelecido no §3º, art. 12, LGPD. Assim, sem prejuízo de que o

procedimento seja indicado como boa prática de governança em proteção de dados pessoais, relevante tanto para tomada de decisão do controlador, quanto para prestação de contas à Autoridade, não poderia ser imposta como obrigação legal.

Neste contexto, mostra-se importante que a Autoridade deixe explícito no estudo que o procedimental indicado e a documentação a ser produzida para lastreá-lo possui caráter, apenas, orientativo aos agentes de tratamento de dados e não obrigacional.

De modo que, os agentes de tratamento de dados tenham a liberdade de, ao avaliarem o risco de reidentificação, escolher a técnica, o modelo, o procedimento e o tipo documental adequado ao contexto do tratamento dos dados objeto da anonimização.

V. CONCLUSÕES

À luz das elucidações acima, esperamos ter contribuído para a consolidação de boas práticas em Proteção de Dados Pessoais e a melhor interpretação para a garantia da eficácia dos direitos estabelecidos pela LGPD.

DANIEL

MACQUARIE University

February, 2024

Brazilian Data Privacy Agency Public Consultation on Anonymization and Pseudonymization for Data Protection

To whom it may concern:

We write in response to the request for public consultation regarding proposed anonymization principles (below referred to as The Proposal) to be adopted by the Brazilian Data Privacy Agency. We are privacy researchers who have been collaborating with Brazilian privacy researchers for a number of years, and who have participated in research related specifically to privacy concerns of the publication of Brazilian Educational Datasets (Instituto Nacional de Estudos e Pesquisas Educacionais, INEP).

We are both established researchers in the privacy field, based at Macquarie University in Sydney (which is ranked amongst the top 150 Universities worldwide for Computer Science and Engineering). Please find below our commentary on the proposals, highlighting a number of concerns based on the very latest research findings in the international privacy community.

Our response:
It is welcome to see that the proposed principles include a continuous monitoring of scenarios, and the proposal to use a risk-based approach for evaluating whether effective techniques have been employed to prevent the re-identification of citizens in the dataset. However the specific metrics proposed and the implementation of anonymization techniques are in opposition to the current scientific understanding of how to provide privacy protections in datasets. We set out the main vulnerabilities of the approach below.

1. **Definition of a re-identification risk:** The Proposal suggests a subjective definition of an upper bound on re-identification risk, without saying exactly what this definition means nor how it relates to the potential harm to citizens. This means that different agencies could use their own definitions, with no scientific foundation for one definition as opposed to another one. Moreover, the risk of re-identification, whilst an important component, does not include the problem of inferring sensitive information about vulnerable groups which is understood in the privacy community to be one of the principal causes of harm.
2. **The Proposal suggests anonymization techniques "suppression, generalization, masking, noise addition, and permutation":** For many years now, it has been convincingly demonstrated that these techniques have inherent vulnerabilities, and are not suitable for privacy protection because of the following:
   - It is not possible to be certain that the correct attributes have been chosen in the anonymisation process because it is never certain what attributes can be assured to be available or not available to a third party. This has led in the past to unexpected privacy breaches and constitutes a severe vulnerability.
   - The safe value of k in the application of k-anonymity cannot be guaranteed: it can be degraded when several datasets are out together, leading to the reconstruction of data.
   - The proposed techniques of generalisation and suppression can be reversed either partially or completely meaning that whatever re-identification risk that has been calculated almost certainly doesn't apply in realistic contexts where reconstruction attacks are likely.
3. We are concerned about the illustrative examples because they are not representative of the size of realistic datasets. For example the 35% risk of re-identification would imply that 17.5 million individuals could be vulnerable to re-identification. This is the number of individuals in the INEP datasets for example.

Yours Sincerely,

Annabelle McIver
Professor Computer Science

Natasha Fernandes
Lecturer in Cyber Security

uma sinergia positiva entre a área jurídica e a área computacional. ","616594":"Em relação a forma do texto, algumas concordâncias nominais precisam de atenção.

Contribuinte: ELDA ELY GOMES DE SOUZA

Número: OP-627681

Data: 22/02/2024 - 13:56

Resumo: "A ANPD acertou ao tratar a anonimização como processo baseado em risco. Considerar a anonimização como um processo absoluto distorce da realidade.","616594":"Sem comentários.

Contribuinte: SAULO SOUZA DE MACEDO

Número: OP-627682

Data: 22/02/2024 - 14:00

Resumo: "A abordagem baseada em processo para a anonimização apresentada pela ANDP demostrasse acertada. Anonimização absoluta não existe.","616594":"Sem comentários.

Contribuinte: ALUIZIO DOS SANTOS CATAO NETO

Número: OP-627698

Data: 22/02/2024 - 14:36

Resumo: ""O texto proposto pela ANPD merece pouquíssimos ajustes, mas as abordagens baseadas em processo demonstram-se adequadas para a realidade".","616594":""Revisas as concordâncias nominais do texto".

Contribuinte: GRAZIELY PIMENTEL MESQUITA

Número: OP-627714

Data: 22/02/2024 - 15:07

Resumo: "As abordagens propostas pela ANPD nos documentos demonstram um nível de alto maturidade da ANPD para tratar do tema.","616594":"Nada a acrescentar.

Contribuinte: MARCUS VINICIUS LOBO COSTA

Número: OP-627988

Data: 23/02/2024 - 10:48

Resumo: "Tendo em vista a quantidade de documentações apresentadas na presente tomada de subsídios, encaminhamos nossas contribuições no formato de anexo para o e-mail: normatizacao@anpd.gov.br, tendo em vista o limite de caracteres disponíveis para escrevermos nestes campos. ","616594":"Tendo em vista a quantidade de documentações apresentadas na presente tomada de subsídios, encaminhamos nossas contribuições no formato de anexo para o e-mail: normatizacao@anpd.gov.br, tendo em vista o limite de caracteres disponíveis para escrevermos nestes campos.

Contribuinte: Asshaias Felippe Eugênio

Número: OP-628146

Data: 23/02/2024 - 14:02

Resumo: "considero o estudo adequado as realidades do mercado","616594":"Nada a adicionar

Contribuinte: WILLIAM DOS SANTOS TEIXEIRA

Número: OP-628456

Data: 26/02/2024 - 11:23

Resumo: "À Autoridade Nacional de Proteção de Dados (ANPD) Ao Senhor Waldemar Gonçalves Ortunho Júnior – Diretor Presidente Atendendo ao Estatuto Social do Instituto Nacional de Proteção de Dados (INPD) e visando apoiar o desenvolvimento do ambiente nacional de proteção de dados pessoais, a observância dos","616594":"A íntegra está sendo encaminhada via e-mail conforme orientações.

Contribuinte: ATILIO AUGUSTO SEGANTIN BRAGA

Número: OP-628463

Data: 26/02/2024 - 11:32

Resumo: "O documento apresenta uma visão realista sobre o contexto da anonimização e pseudoninimização","616594":"Nada a declarar

Contribuinte: MAYARA JESSICA DA SILVA

Número: OP-628630

Data: 26/02/2024 - 17:39

Resumo: "A minuta apresentada está de acordo com a realidade existente no mercado.","616594":"Nada a adicionar.

Contribuinte: JONAS DA CONCEICAO NASCIMENTO PONTES

Número: OP-628632

Data: 26/02/2024 - 18:13

Resumo: "As abordagens propostas no estudo são realistas, o que demonstra uma maturidade do órgão no tema.","616594":"nada a adicionar.

Contribuinte: JESSYE BARROSO VALENTE

Número: OP-628664

Data: 27/02/2024 - 04:55

Resumo: "Envio em anexo duas cartas de pesquisadores da área de privacidade de dados pessoais referentes à contribuição encaminhada por meio da Plataforma Participa Mais Brasil sobre a "Consulta à Sociedade sobre a minuta do Guia de Anonimização e Pseudonimização para a Proteção de Dados Pessoais".","616594":"Envio em anexo duas cartas de pesquisadores da área de privacidade de dados pessoais referentes à contribuição encaminhada por meio da Plataforma Participa Mais Brasil sobre a "Consulta à Sociedade sobre a minuta do Guia de Anonimização e Pseudonimização para a Proteção de Dados Pessoais".

Contribuinte: GABRIEL HENRIQUE LOPES GOMES ALVES NUNES

Número: OP-629089

Data: 27/02/2024 - 16:00

Resumo: "Parabenizamos a ANPD pelo trabalho e iniciativa e entendemos, inclusive, que houve acerto em não tratar o tema apenas sob a perspectiva jurídica. Enviaremos as contribuições para normatizacao@anpd.gov.br.","616594":"Diante da limitação de caracteres, enviaremos as contribuições para normatizacao@anpd.gov.br.

Contribuinte: Anderson Antonio Monteiro Mendes

Número: OP-630235

Data: 28/02/2024 - 09:28

Resumo: "O IAB Brasil, apresenta a seguir suas contribuições acerca do estudo preliminar. A contribuição em sua íntegra foi enviada para o e-mail disponibilizado pela autoridade. ","616594":"anexo enviado por e-mail.

Contribuinte: Beatriz Falcão Vilarinho Fernandes

Número: OP-632176

Data: 28/02/2024 - 10:15

Resumo: "As técnicas do item 81 podem ser utilizadas p/ anonimização de dados, diferenciando-se da pseudonimização pela reversibilidade. Não recomendamos a sua listagem como se apenas se referissem à pseudonimização. Mesmo raciocínio acompanha págs. 19 e 23 cujas metodologias podem ser unificadas.","616594":"Sugere-se mencionar a diferença entre dado anônimo e anonimizado, tópico 4.2. As fotos do ex. de técnicas de anonimização de imagem (tarja apenas no olho) devem cobrir a face totalmente. O conceito está correto, mas a imagem não. O número de caracteres para contribuição (300) é insuficiente.

Contribuinte: Alessandra Rigueti Barcellos

Número: OP-632211

Data: 28/02/2024 - 12:11

Resumo: "Encaminhada via email a contribuição elaborada conjuntamente pela FEBRABAN e ABECS, a fim de colaborar com a Consulta à Sociedade - Estudo Preliminar - Anonimização e pseudonimização para proteção de dados.","616594":"Encaminhada via email a contribuição elaborada conjuntamente pela FEBRABAN e ABECS, a fim de colaborar com a Consulta à Sociedade - Estudo Preliminar - Anonimização e pseudonimização para proteção de dados.

Contribuinte: Arthur Gomez Villar Maruca

Número: OP-632319

Data: 28/02/2024 - 14:58

Resumo: "A regulamentação deve prever medidas de mitigação de risco no tratamento de dados especialmente pelo setor privado, como (i) impossibilidade de usar anonimização para chancelar tratamentos ilícitos ou que não cumprem com a LGPD; (ii) parâmetros rigorosos para o compartilhamento de dados anonimizados","616594":"A distinção entre

dados anônimos e anonimizados é essencial. A regulamentação não deve ser usada para isentar o agente de tratamento de suas responsabilidades, mas proteger o titular de dados. A anonimização deve ser considerada uma operação de tratamento, com especial atenção a reidentificação.

Contribuinte: LUCAS MARTHO MARCON

Número: OP-632328

Data: 28/02/2024 - 15:07

Resumo: "Contribuições TIM S/A - Considerando que o conteúdo das contribuições ultrapassa o número de caracteres permitidos, enviamos as nossas sugestões através do e-mail normatizacao@anpd.gov.br.","616594":"Contribuições TIM S/A - Considerando que o conteúdo das contribuições ultrapassa o número de caracteres permitidos, enviamos as nossas sugestões através do e-mail normatizacao@anpd.gov.br.

Contribuinte: ROBERTA ARNOSO QUINTANEIRO

Número: OP-632377

Data: 28/02/2024 - 16:39

Resumo: "2.1O que “meio técnico razoável”?Como seria esse "dado auxiliar"?3.1Informar ao titular que uma das finalidades seria anonimizar?Quais hipóteses isso seria viável para controlador?3.2 Como será compatível e ser além daquilo que o dado foi originalmente coletado 3.2.1Esclarecer grau de anonimização","616594":"Não há sugestões

Contribuinte: Bruna Tais Sambugaro

Número: OP-632409

Data: 28/02/2024 - 17:44

Resumo: "O Estudo Preliminar está claro e objetivo.Nota-se uma subjetividade intrínseca quanto à padronização da forma de anonimização,conforme mostrado nos estudos de casos. Consequentemente,nos cabe seguir as instruções gerais,onde faz-se necessário analisar a finalidade do dado pessoal.","616594":""a anonimização não deve se restringir à discussão de técnicas, mas sim uma abordagem mais ampla baseada em processo."Sugestão: Criar fluxo referente a execução da anonimização, atribuindo responsabilidades na execução da técnica adotada, evidências e monitoramento até a gestão contínua de riscos.

Contribuinte: VIVIAN MEYER MARSHALL DE ALBUQUERQUE

Número: OP-632420

Data: 28/02/2024 - 18:30

Resumo: "CNseg: Anonimização não deve ser considerada tratamento de dado pessoal; análise da identificabilidade do dado deve ser feita apenas com meios detidos pelo controlador; necessidade de diretrizes claras de RRA/RRM; e controlador deve avaliar a metodologia mais adequada ao processo de pseudonimização.","616594":"Oficio PRESI-033/2024 será enviado para o e-mail normatizacao@anpd.gov.br.

Contribuinte: ANA BEATRIZ CONDE GALVAO

Número: OP-632997

Data: 01/03/2024 - 16:03

Resumo: "Em razão da limitação de caracteres (300), a integralidade das contribuições de Leonardi Advogados foi enviada em documento separado (PDF) para o e-mail indicado (normatizacao@anpd.gov.br)","616594":"Sugerimos que, em consultas públicas futuras, não haja tamanha limitação de caracteres, ainda mais considerando a complexidade do tema e o número de páginas dos documentos apresentados pela própria ANPD.

Contribuinte: Marcel Leonardi

Número: OP-633677

Data: 05/03/2024 - 13:31

Resumo: "O Sistema FIEMG, em nome do Grupo de Trabalho instituído com a finalidade de analisar as disposições legais e regulatórias sobre proteção de dados, apresenta anexo as contribuições sobre o Estudo Preliminar - Anonimização e pseudonimização para proteção de dados.","616594":"Enviado em 05/03/2024.

Contribuinte: HORTENCIA RICARTE DE OLIVEIRA PAIZANTE

Número: OP-635209

Data: 11/03/2024 - 13:16

Resumo: "Encaminhado material complementar em nome da Associação Brasileira de Medicina Diagnóstica (ABRAMED) por meio do e-mail: normatizacao@anpd.gov.br.","616594":"Encaminhado material complementar em nome da Associação Brasileira de Medicina Diagnóstica (ABRAMED) por meio do e-mail: normatizacao@anpd.gov.br.

Contribuinte: LUIZA TEOTONIO CIPRIANO SILVA

Número: OP-635359

Data: 11/03/2024 - 16:35

Resumo: "CONEXIS BRASIL DIGITAL: as contribuições foram enviadas por conexis@conexis.org.br (título: Envio de Contribuições Conexis Brasil Digital - Consulta à Sociedade sobre o Guia de Anonimização e Pseudonimização) ao e-mail normatizacao@anpd.gov.br no dia 28/02/24 às 17:40hrs.","616594":"CONEXIS BRASIL DIGITAL: as contribuições foram enviadas por conexis@conexis.org.br (título: Envio de Contribuições Conexis Brasil Digital - Consulta à Sociedade sobre o Guia de Anonimização e Pseudonimização) ao e-mail normatizacao@anpd.gov.br no dia 28/02/24 às 17:40hrs.

Contribuinte: Jonathan Naves Palhares

Número: OP-635650

Data: 12/03/2024 - 09:44

Resumo: "TF: Recomendamos critérios melhor definidos para teste de risco de identificabilidade; aprimorar Apêndice II para anonimização de imagens, pois técnica adotada parece insuficiente; e esclarecer se dado pode ser considerado anonimizado para um agente, caso outro não relacionado puder reidentificá-lo.","616594":"TF: Recomenda-se que a ANPD publique parte do estudo como diretriz de boas práticas (ex: técnicas), e outra como resolução vinculante (ex: a avaliação da possibilidade de reidentificação deve considerar encargos derivados da força de trabalho, custos e tempo exigidos).

Contribuinte: Julia Parizotto Menzel

Número: OP-636934

Data: 13/03/2024 - 21:56

Resumo: "Encaminhamos contribuições da Petrobras pelo e-mail [redacted] para normatizacao@anpd.gov.br. Agradecemos a oportunidade de participar.","616594":"Encaminhamos contribuições da Petrobras pelo e-mail [redacted] para normatizacao@anpd.gov.br. Agradecemos a oportunidade de participar.

Contribuinte: ELTON LUIS MITIDIERI ARNAUD

Número: OP-636960

Data: 14/03/2024 - 08:05

Resumo: "A camara-e.net cumprimenta a ANPD pela iniciativa. O Estudo traz o entendimento de que a anonimização pode ser uma forma de garantir privacidade e proteção de dados. Todavia, ainda há espaço para aperfeiçoamentos, apresentados em documento enviado por e-mail.","616594":"A camara-e.net enviará a íntegra de suas contribuições via e-mail.

Contribuinte: THAIS HELENA VACCARI COVOLATO

Número: OP-636975

Data: 14/03/2024 - 08:44

Resumo: :"A Zetta, associação sem fins lucrativos que representa empresas de tecnologia constituídas como plataformas de serviços financeiros digitais, enviou o anexo com a totalidade de suas contribuições sobre o Estudo Preliminar ao e-mail normatizacao@anpd.gov.br.","616594":"A Zetta, associação sem fins lucrativos que representa empresas de tecnologia constituídas como plataformas de serviços financeiros digitais, enviou o anexo com a totalidade de suas contribuições sobre o Estudo Preliminar ao e-mail normatizacao@anpd.gov.br.

Contribuinte: Laryssa de Menezes Silva

Número: OP-637010

Data: 14/03/2024 - 09:15

Resumo: "Encaminhado material complementar em nome da Associação Nacional dos Hospitais Privados (ANAHP) por meio do e-mail: normatizacao@anpd.gov.br, em 14/03.2024. Título do e-mail: Contribuições da ANAHP para a Consulta à Sociedade sobre Guia de Anonimização e Pseudonimização da ANPD","616594":"Encaminhado material complementar em nome da Associação Nacional dos Hospitais Privados (ANAHP) por meio do e-mail: normatizacao@anpd.gov.br, em 14/03.2024. Título do e-mail: Contribuições da ANAHP para a Consulta à Sociedade sobre Guia de Anonimização e Pseudonimização da ANPD

Contribuinte: MAURICIO THOME NEGREIRA

Número: OP-637471

Data: 14/03/2024 - 12:46

Resumo: "Sugerimos incluir esclarecimentos sobre: (i) a possibilidade de utilização de pseudonimização como estratégia de ‘’minimização de dados’’ e proteção de dados

pessoais; e (ii) se a implementação de técnicas de pseudonimização pode ter efeitos sobre as obrigações dos agentes de tratamento.","616594":"A anonimização deve ser compreendida como uma estratégia de mitigação de riscos e proteção de dados, e não como uma operação de tratamento de dados. Sugerimos que o Estudo esclareça adequadamente as diferenças entre as duas atividades, a fim de não confundir os agentes de tratamento.

Contribuinte: GABRIELA RIBEIRO GOMES SOTOMAYOR

Número: OP-637474

Data: 14/03/2024 - 12:58

Resumo: "BBL Adv - Sugerimos esclarecer sobre a identificação de dados anonimizados a partir de informações em posse de terceiros, bem como pelo cruzamento de dados do titular disponíveis publicamente, a fim de aprimorar a análise do risco de reidentificação e auxiliar na escolha da técnica de anonimização. ","616594":"BBL Adv – Sugerimos que o Estudo aborde a necessidade de os agentes de tratamento analisarem as implicações do uso de técnicas de anonimização e pseudonimização aos titulares de dados, garantindo que o processo atenda ao seu propósito sem comprometer as garantias e os direitos dos titulares.

Contribuinte: Anna Luiza da Silva

Número: OP-637497

Data: 14/03/2024 - 13:57

Resumo: "Prezados/as, Em razão da limitação de caracteres na Plataforma+ Brasil, as contribuições da Associação Brasileira de Internet - ABRANET foram enviadas por e-mail pelo endereço de e-mail [redacted] no dia 14/03/2024, às 14h21. Atenciosamente, ABRANET.","616594":"Prezados/as, Em razão da limitação de caracteres na Plataforma+ Brasil, as contribuições da Associação Brasileira de Internet - ABRANET foram enviadas por e-mail pelo endereço de e-mail caroline@abranet.org.br, no dia 14/03/2024, às 14h21. Atenciosamente, ABRANET.

Contribuinte: SILAS CARDOSO DE SOUZA

Número: OP-637505

Data: 14/03/2024 - 13:57

Resumo: "Contribuições enviadas por email","616594":"Contribuições enviadas por email

Contribuinte: FERNANDA SOARES ROSA

Número: OP-637570

Data: 14/03/2024 - 14:51

Resumo: "Nessa oportunidade, a ANBC vem apresentar a sua contribuição à ANPD, reiterando seus cumprimentos pela iniciativa de consultar e colher subsídios de todos os setores interessados com vistas a contribuir para a atuação da Autoridade em torno do tema.","616594":"As considerações da Associação Nacional dos Bureaus de Crédito será enviada por e-mail, tendo em vista a limitação de número de caracteres nessa plataforma, dentro do prazo concedido.

Contribuinte: Patrícia Leal Ferraz bove

Número: OP-637569

Data: 14/03/2024 - 14:52

Resumo: "O LAPIN sugere o estabelecimento de: Agenda de revisão periódica sobre estado da arte, linhas de capacitação e pesquisa, formas de parceria com a comunidade científica. Diretrizes e metodologia de fiscalização. Materiais de conscientização de titulares e orientações para agentes de pequeno porte","616594":"Elaboramos um documento com considerações adicionais e detalhamento das sugestões indicadas no primeiro campo. Enviaremos o documento por e-mail.

Contribuinte: Luiza Xavier Morales

Número: OP-637628

Data: 14/03/2024 - 15:21

Resumo: "CNC: Itens 29, 30 e 31 do Estudo: O dado anonimizado deixa de ser dado pessoal e dispensa conformidade com a LGPD. Se o tratamento anterior possuía alguma irregularidade, após a anonimização, os dados anonimizados não precisarão ser eliminados, pois não haverá mais tratamento de dados pessoais. ","616594":"Item 34 doEstudo: A anonimização não é uma finalidade que legitima o tratamento de dados pessoais, e sim uma medida de segurança e gestão de riscos. Na fase inicial de coleta de dados, o controlador não tem o dever de informar uma futura e eventual anonimização como uma das finalidades do tratamento

Contribuinte: CAMILA DA COSTA VIEIRA BLANCO

Número: OP-637870

Data: 14/03/2024 - 16:47

Resumo: "Em nome do Baptista Luz Advogados, encaminharei no e-mail da ANPD as contribuições do escritório para a Consulta Pública envolvendo o Estudo Preliminar de Anonimização e pseudonimização para proteção de dados. ","616594":"Anexo enviado por e-mail.

Contribuinte: FERNANDO BOUSSO

Número: OP-637880

Data: 14/03/2024 - 16:59

Resumo: "Diante do direito à anonimização, previsto na LGPD, a ANPD deve proporcionar meios para que as técnicas e ferramentas para esses fins sejam de fato acessíveis, para que sirva à soberania popular digital, e sua aplicação não se limite às relações de produção e consumo.","616594":"Diante do direito à anonimização, previsto na LGPD, a ANPD deve proporcionar meios para que as técnicas e ferramentas para esses fins sejam de fato acessíveis, para que sirva à soberania popular digital, e sua aplicação não se limite às relações de produção e consumo.

Contribuinte: ALEXEI JOSE ZARATINI

Número: OP-637891

Data: 14/03/2024 - 17:12

Resumo: "A ABIPAG destaca como os principais pontos: Uniformizar definições, Não responsabilizar pela Reidentificação, Atribuir natureza de recomendação à sugestão das etapas de pseudonimização, e possibilitar a automatização completa da anonimização","616594":"Para uma compreensão mais específica dessas propostas, a ABIPAG encaminha a tabela anexa, em que cada ponto será abordado em detalhe.

Contribuinte: Nathalia Rodrigues Bittencourt Martins Oliveira de Menezes

---

Número: OP-637900

Data: 14/03/2024 - 17:26

Resumo: "Gostaria de contribuir com o meu artigo "Anonimização, 'Venire Contra Factum Proprium' e Relatório dos Riscos de Reidentificação", publicado pela Editora RT, In: Estudos Sobre Privacidade e Proteção de Dados. São Paulo, 2021, pp. 155-186. ISBN: 978655991849.

","616594":"Abordo a importância da transparência dos agentes não somente diante do conteúdo já exposto pela ANPD em seu guia, mas também pelo princípio de direito civil da vedação ao comportamento contraditório no âmbito das contratações (venire contra factum proprium).

Contribuinte: Clarissa Ignacio jorge luz

Número: OP-637913

Data: 14/03/2024 - 17:42

Resumo: "O time CIR Samsung sauda a ANPD pela publicização da consulta pública sobre o Estudo Preliminar sobre Anonimização e Pseudonimização sob a LGPD. A análise destaca a complexidade da anonimização de dados e a necessidade de diretrizes claras. Detalhes completos serão enviados por e-mail.","616594":"Solicitamos à ANPD que futuras extensões de prazo sejam comunicadas com maior antecedência. Informar no último dia do prazo original dificulta o planejamento e a organização das partes interessadas. Detalhes completos serão enviados por e-mail.

Contribuinte: Paulo Henrique Atta Sarmento

Número: OP-637920

Data: 14/03/2024 - 18:03

Resumo: :"Venho, em nome da Associação Brasileira de Planos de Saúde - ABRAMGE e da Associação Brasileira de Planos Odontológicos - SINOG, na figura de sua Advogada e DPO, sinalizar que encaminhamos nossas contribuições via e-mail (lgpdsistema@abramge.com.br), em virtude da restrição de caracteres.","616594":"Venho, em nome da Associação Brasileira de Planos de Saúde - ABRAMGE e da Associação Brasileira de Planos Odontológicos - SINOG, na figura de sua Advogada e DPO, sinalizar que encaminhamos nossas contribuições via e-mail (lgpdsistema@abramge.com.br), em virtude da restrição de caracteres.

Contribuinte: Camila Castioni Secundino

Número: OP-637956

Data: 14/03/2024 - 19:56

Resumo: "Contribuições, em nome da Daniel Advogados, referentes aos itens 3.1.1, parágrafo 37 (aplicabilidade da LGPD ao processo de anonimização); Item 3.1.2 (risco de reidentificação); Item 3.1.3 (meios próprios); e Item 3.2.2 (gestão do risco), do Estudo

Preliminar em anexo. ","616594":"Contribuições, em nome da Daniel Advogados, referentes aos itens 3.1.1, parágrafo 37 (aplicabilidade da LGPD ao processo de anonimização); Item 3.1.2 (risco de reidentificação); Item 3.1.3 (meios próprios); e Item 3.2.2 (gestão do risco), do Estudo Preliminar em anexo.

Contribuinte: Nuria López Cabaleiro Suárez

Número: OP-637964

Data: 14/03/2024 - 20:41

Resumo: "Incluir quadro exemplificativo itens 13 -15. Conveniência da anonimização, não será exigida do controlador (item 22). Item 58 se efetivamente ocorrer a anonimização, não haverá aplicação da legislação. Item 71, L-Diversidade e a T-Proximidade. Item 3.2 citar Dados Sintéticos e Princípio da Exaustão.","616594":"Com objetivo de introduzir o tema à sociedade e ao leitor, o presente estudo poderia mencionar questões relacionadas ao uso da criptografia homomórfica, que permite trabalhar com dados criptografados sem a necessidade de descriptografá-los, minimizando a possibilidade de exposição das informações.

Contribuinte: LUCAS GRANDINI ARTHUSO

Número: OP-637977

Data: 14/03/2024 - 21:50

Resumo: "Escopo jurídico: Entende-se que a anonimização não deveria ser considerada como uma operação de tratamento autônoma, mas como uma medida técnica acessória destinada a garantir a conformidade e segurança de uma base de dados. O anexo contendo a fundamentação será enviada ao email indicado.","616594":"Escopo Técnico. A ANPD poderia apresentar um framework para guiar a decisão do nível de anonimização a ser aplicada, levando em conta o equilíbrio entre risco e utilidade. Ou seja, regras e parâmetros claras para diferentes situações, tipos de dados ou metas de análise, incluindo exemplos práticos.

Contribuinte: Samanta Santos de Oliveira