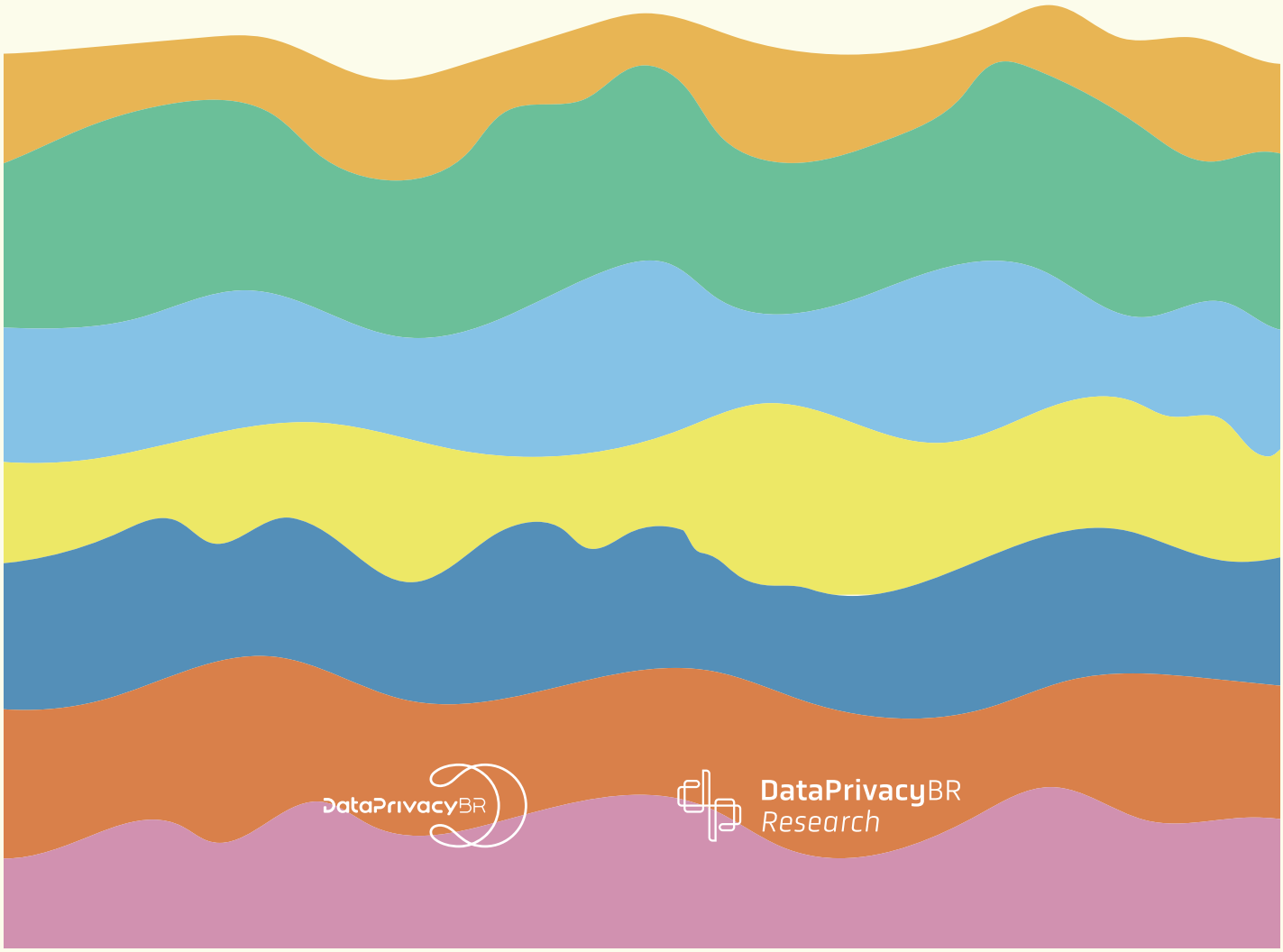
Entrelinhas

Explorando a Privacidade e Proteção de Dados em Comunidade

Gedeão Felipe Ferreira de França e
Pedro Bastos Lobo Martins (orgs.)



Ficha técnica

ORGANIZAÇÃO
Gedeão França e Pedro Martins

DIREÇÃO DE ARTE e DIAGRAMAÇÃO
Roberto Junior

PRODUÇÃO EDITORIAL
DPBR - Data Privacy Brasil

COMO REFERENCIAR
FRANÇA, Gedeão Felipe Ferreira de; MARTINS, Pedro Bastos Lobo (orgs.). *Entrelinhas*: Explorando a Privacidade e Proteção de Dados em comunidade. São Paulo: Data Privacy Brasil. 2024. Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2024/01/entrelinhas-vf.pdf. Acesso em: dd mmm aaaa.

IMPRENSA
Para esclarecimentos sobre o documento e entrevistas, entrar em contato com a Data Privacy Brasil pelo e-mail imprensa@dataprivacybr.org

ENTRELINHAS

Institucional

A Data Privacy Brasil é uma organização que nasce da união entre uma escola e uma associação civil em prol da promoção da cultura de proteção de dados e direitos digitais no Brasil e no mundo. Para isso, com o apoio de uma equipe multidisciplinar, realizamos formações, eventos, certificações, consultorias, conteúdos multimídia, pesquisas de interesse público e auditorias cívicas para promoção de direitos em uma sociedade datificada marcada por assimetrias e injustiças. Por meio da educação, da sensibilização e da mobilização da sociedade, almejamos uma sociedade democrática onde as tecnologias estejam a serviço da autonomia e dignidade das pessoas.

DIRETORES
Bruno Bioni, Rafael Zanatta e Mariana Rielli

COORDENAÇÃO
Carla Rodrigues, Jaqueline Pigatto, Pedro Martins. Pedro Saliba e Victor Barcellos

CURSOS E NOVOS NEGÓCIOS
Eduarda Costa, Gedeão França, Otávio Almeida e Pedro Henrique Martins

PESQUISA
Eduardo Mendonça, Gabriela Vergili, Júlia Mendonça, Horrara Moreira, Louise Karczeski, Paula Guedes, Vinicius Silva e Nathan Paschoalini

COMUNICAÇÃO E MARKETING
Alicia Lobato, Rafael Guimarães, Rafael Regatieri, Isabela Santos, Isabelle Gomes e Roberto Junior

ADM E FINANCEIRO & PODCAST
Rodolfo Rodrigues, Matheus Arcanjo e João Vicente

ENTRELINHAS

Autores

Bárbara Steffens
Doutora e Mestra em Direito pela Universidade de Santa Crus do Sul – UNISC, pós-graduada em Especialista em Proteção de Dados: LGPD e GDPR, pela Fundação Escola Superior do Ministério Público do Rio Grande do Sul. Especialista em Advocacia Contratual e Responsabilidade Civil pela Escola Brasileira de Direito – Ebradi. Advogada. E-mail: barbarakunde@gmail.com.

Bruna Cruz
Advogada, Líder da Embaixada Data Brasília, Pós Graduada em Direito Empresarial pelo IBMEC, MBA em Digital Business pela USP, Encarregada de Proteção de Dados no IgesDF, Consultora em Privacidade na DisrupMind e diversos cursos em Proteção de Dados pelo Data Privacy BR.

Carmen Arriagada
Sócia de Pereira Gionédis Advogados. Líder da Embaixada Data Curitiba. Pós-graduada em Direito Digital pela Pontifícia Universidade Católica do Paraná. Formação em Proteção de Dados pela Data Privacy Brasil. Certificada em Proteção de Dados pela Fundação Getúlio Vargas. Especialista com MBA em Direito da Empresa e Economia pela Fundação Getúlio Vargas. Especialista em Direito Civil pelo Instituto Brasileiro de Estudos Jurídicos - IBEJ. Especialista em Direito Contratual pela Pontifícia Universidade Católica do Paraná. Bacharel em Direito pela Universidade Federal do Paraná. Membro atuante do CESA - Centro de Estudos de Sociedades de Advogados. Membro da Comissão de Arbitragem da OAB-PR. Membro da Comissão de Direito Digital e Proteção de Dados da OAB/PR. Coordenadora do GPD Direito Digital e Eleições junto à Comissão de Direito Digital e Proteção de Dados da OAB/PR.

Cristyane Bastos
Encarregada Pelo Tratamento de Dados Pessoais nomeada. Advogada, sócia no escritório Aguilar Advogados. Bacharel em Direito UFPA. Pós Graduação em Direito Processual UNISUL. MBA-FVG Direito Empresarial. Compliance (INSPER). Compliance em Lei Geral de Proteção de Dados (LEC) - Certificação Profissional de Compliance em Proteção de Dados - CPD-PD. Certificação internacional Information Privacy Manager - CIPM IAPP, Certificação internacional CDPO IAPP, Discente do Curso Superior de Tecnologia em Segurança da Informação - PUCMINAS. Curso de Privacidade e Proteção de Dados Avançado Data Privacy Brasil. Membro do Comitê Jurídico da ANPPD®, IAPP Member, Membro ANADD.

Daiane Conde
Atualmente na Equipe de Privacidade da Oi S.A. Fundadora do Clube do Livro do Clube Data. Líder da Embaixada Data Rio de Janeiro. Formação em Direito pela Universidade Federal Fluminense.

Fernanda Ratzkowski
Graduada em Relações Internacionais na ESPM e em Direito na UFRGS. Tem pós-graduação em Direitos Humanos e atualmente é pós-graduanda em Direito Contratual, Responsabilidade Civil e Direito Imobiliário, ambos pela PUCRS. Foi aprovada no XXXVI Exame da Ordem. Possui experiência na elaboração de projetos de adequação à LGPD e na confecção de pareceres consultivos sobre o tema.

Fernando Vasconcelos
DPO e advogado do time de Legal do Rei do Pitaco, sportech brasileira do setor de Fantasy Games. Pós graduado em Direito Desportivo (IIDD) e Compliance (FGV). Ex-aluno da Turma 23 do Curso de Privacidade e Proteção de Dados do Data Privacy Brasil.

Franklin Jeferson
Especialista de privacidade e proteção de dados na ANPD. Certificações ABNT Lead Implementer 27701; EXIN DPO; Introduction to Cybersecurity CISCO; Gestor de Dados SERPRO; DPO Serpro; Information Security & Privacy Risk Manager - TIEXAMES; Pós graduado LLM em LGPD/GDPR - FMP/Universidade de Lisboa; Pós graduado em LGPD - Legale.

Juliana Brasileiro
Advogada, Líder da Embaixada Data Campina Grande, Pós-graduada em Direito Digital e Proteção de Dados pelo Instituto de Direito Privado, em Direito da Medicina pela Universidade de Coimbra – PT e em Direito Médico e da Saúde pela UNIFACISA, sócia-fundadora da CABRAL & BRASILEIRO advocacia e consultoria, sócia-fundadora da DATA SAÚDE Privacidade e Proteção de Dados.

Julie Borges
Advogada, Legal Designer, Líder da Embaixada Data Fortaleza e apaixonada por inovação. Estudiosa nas áreas de Inteligência Artificial, Data Driven Decisions, Privacidade e Proteção de Dados. Pós-graduanda em Direito, Tecnologia e Proteção de Dados pela Universidade de Fortaleza (UNIFOR).

Luciano Escobar
Advogado, Pós-graduado em Direito Educacional pela Verbo Jurídico, Pós-graduando em Proteção de Dados: LGPD & GDPR (LLM Internacional Brasil - Portugal) pela Fundação Escola Superior do Ministério Público do RS, Membro da Comissão Especial de Proteção de Dados e Privacidade da OAB/RS, do Grupo de Estudos em LGPD da OAB/RS e Membro da Comissão Permanente de Direito Digital e LGPD da FEDERASUL, Conselheiro titular do CEDECON - Conselho Estadual de Defesa do Consumidor do RS.

Luis Acioly
Head de Privacidade e Proteção de Dados do Laboratório de Inovação e Direitos Digitais da UFBA – LABID[2]. Curador Jr. de Pesquisa junto ao Grupo de Estudos em Tecnologia, Informação e Sociedade da UNIFOR – GETIS. Graduando em Direito pelo UniRuy.Pesquisador no Grupo "Conversas Civilísticas" - UFBA/CNPq. Treinee Jurídico no Núcleo de Tecnologia e Governança no Chezzi Advogados.

Luiza Teotônio
Advogada do Escritório Machado Nunes, integrante do time de Inovação. Especialista em Direito Digital e Proteção de Dados (ESA-OAB-SP), Data Protection Officer pela EXIN, Pós-graduanda em Direito Empresarial: Estruturas Societárias, Contratos e Compliance pela Faculdade de Direito de Ribeirão Preto (USP).

Mauricio Negreira
Advogado do Escritório Machado Nunes, integrante do time de Inovação. Especialista em Direito Civil pela Universidade Presbiteriana Mackenzie. Pós-Graduando em Tecnologia para Negócios, IA, Data Science e BigData pela Puc-RS; Certificado pelo EXIN em Privacy and Data Protection - Essentials based on LGPD.

Pollyana Moreira
Graduação em Artes pela UFJF e Pedagogia. Especialização em Gestão de Documentos e Informações e Especialização em Direitos Humanos. Técnica em Arquivo no IF Sudeste MG. Encarregada pelos Dados Pessoais, membro do Comitê de Segurança da Informação e Presidente do Comitê Gestor de Proteção de Dados todos junto ao IF Sudeste MG. Certificação de DPO (Data Protection Officer) com foco na LGPD (Lei Geral de Proteção de Dados Pessoais), ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27701 pela Tradius.

Thúlio Silveira
DPO Coordenador da equipe de Proteção de Dados na Bio Extratus Cosméticos Naturais, especialista em Segurança da Informação, cibersegurança, aluno Data Privacy, membro do GT LGPD da Abhipec Brasil.

Vanessa Santos
Mestre em Planejamento e Análise de Políticas Públicas - Lei Geral de Proteção de Dados (UNESP). Especialista em Contratos (FAAP) e Direito do Consumidor (ESA/OAB). Certificações: Certified Information Privacy Manager (CIPM/IAPP) e Data Privacy Brasil; Pesquisadora Direto UNESP sobre mobilização da Justiça no período pandêmico. Head de Proteção e Privacidade de Dados e Propriedade Intelectual do escritório Trevisan, Pereira e Carmona . Professora com graduações em História (UNESP) e Direito (UNAERP).

“Se eu vi mais longe, foi por estar sobre ombros de gigantes.”

ISAAC NEWTON

ENTRELINHAS

Sumário

SEÇÃO I
Cultura de Privacidade e Design 16

Como e Por Que Difundir a Cultura de Privacidade e Proteção de Dados? 17
Daiane Conde

Privacy by Design 23
Julie Borges

SEÇÃO II
Aplicação da LGPD em Contextos Específicos 29

Dados de saúde e as bases legais para tutela da saúde tendo o paciente com a centralidade da proteção dos dados pessoais 30
Bárbara Steffens

A Lei Geral de Proteção de Dados Pessoais no Contexto das Escolas Particulares 38
Luciano Escobar

A Lei Geral de Proteção de Dados - Lei Nº 13.709/2018 –, E a importância da inserção do princípio da não discriminação como contribuição para uma sociedade mais justa 53
Vanessa Santos

SEÇÃO III
Privacidade e Proteção de Dados na Infância e Adolescência 66

Hipóteses legais aplicáveis ao tratamento de dados de crianças e adolescentes **67**
Juliana Brasileiro

Utilização da tecnologia de reconhecimento facial de crianças e adolescentes no ambiente escolar e os cuidados a serem observados **75**
Franklin Jeferson, Pollyana Moreira

SEÇÃO IV
Segurança da Informação e proteção de dados **83**

Segurança de Informação - cuidados básicos **84**
Carmen Arriagada

Desafios, Estratégias e Procedimentos Práticos para Proteção dos Dados, Segurança das Informações **92**
Thúlio Silveira

Gestão de incidentes de segurança e a importância da comunicação transparente em uma estrutura corporativa de proteção de dados **98**
Fernando Vasconcelos

SEÇÃO V
Normas e Governança em Privacidade 102

Análise da norma ABNT NBR ISO/IEC 29151 e seus benefícios para Programas de Governança em Privacidade 103
Bruna Cruz

As normas corporativas globais como mecanismo de comprovação de garantias nas transferências internacionais de dados pessoais 115
Fernanda Ratzkowski

SEÇÃO VI
Responsabilidade Civil e Proteção ao Consumidor 127

Pontos de contato entre a Responsabilidade Civil no Código de Defesa do Consumidor (CDC) e a Lei Geral de Proteção de Dados (LGPD) 128
Luiza Teotônio, Mauricio Negreira

SEÇÃO VII
Regulação de novas tecnologias 135

Algorithmic Impact Assessment (AIA) e regulação de Inteligência Artificial 136
Luis Acioly

Accountability, da teoria à prática: casos de (in)sucesso prestando contas e gerenciando risco jurídico-regulatório 142
Cristyane Bastos

Apresentação

Gedeão França

Advogado, Young Leader 2022, Forbes BLK Member, pós-graduado em Direito Civil e Processo Civil pela Universidade Maurício de Nassau e pós-graduando em Direito Digital e Proteção de Dados pelo Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP). Community Manager Pleno da Data Privacy Brasil. Pesquisador e Assistente de Pesquisa no Centro de Direito, Internet e Sociedade do IDP (CEDIS) e IDP Privacy Lab. Secretário-adjunto da Comissão de Privacidade e Proteção de Dados da OAB-PE.

É com grande alegria que apresento este e-book criado para oferecer a você uma visão detalhada do que foi dialogado ao longo de 4 edições do Data Talks em 2023. Uma verdadeira consolidação da Comunidade da Data.

O Data Talks surgiu com a ideia de dar voz e visibilidade aos membros da Comunidade Data. Desde a concepção do projeto, gostaríamos de oferecer um espaço de membros para membros, onde todos pudessem compartilhar os seus conhecimentos e aprendizados. Pois, acreditamos ferreamente que as conexões e eventuais oportunidades se dão em espaços de troca.

Em cada edição convidamos 5 membros da nossa comunidade para contribuir através de apresentações curtas e cuidadosamente preparadas sobre uma ampla gama de assuntos abordados em nossas formações e nas suas atividades práticas profissionais. Tais membros não só ocupam espaços relevantes no Setor Empresarial, Terceiro Setor, Setor Governamental, Comunidade Científica e Tecnológica, como também contam com um elevado grau de amadurecimento frente aos assuntos que atravessam a área de privacidade, proteção de dados e regulação de novas tecnologias. Além disso, o corpo de autores desse trabalho é composto de indivíduos de várias cidades do Brasil.

Estamos muito felizes por reunir profissionais que admiramos e respeitamos tanto! Guardo com imensa alegria a lembrança de como, em cada edição, o espírito de comunidade se manifestou de maneira marcante.

Inúmeras contribuições, dúvidas e provocativas discussões deram origem ao significativo título que hoje conhecemos como "*Entrelinhas: Explorando a Privacidade e Proteção de Dados em comunidade*." De pronto, muito surpreendeu a todos internamente, pois o Data Talks foi o primeiro resultado palpável dos trabalhos que estamos desenvolvendo na nossa Comunidade Data.

Ao longo destas páginas, com uma visão multissetorial, você descobrirá estratégias, dicas valiosas e informações essenciais sobre Cultura de Privacidade e Design, Aplicação da LGPD em Contextos Específicos, Privacidade e Proteção de Dados na Infância e Adolescência, Segurança da Informação e proteção de dados, Normas e Governança em Privacidade e Responsabilidade Civil e Proteção ao Consumidor.

Este e-book foi cuidadosamente elaborado para proporcionar a você uma experiência enriquecedora, transformadora e prática, permitindo que você absorva o conteúdo para incorporar nas suas atividades profissionais.

Vamos começar esta jornada juntos!

Prefácio

Rafael Zanatta

Diretor da Associação Data Privacy Brasil de Pesquisa. Doutor pelo Instituto de Energia e Ambiente da Universidade de São Paulo, com período de estudos no Instituto de Direito da Informação da Universidade de Amsterdam. Mestre em Filosofia e Teoria Geral do Direito pela Faculdade de Direito da USP e em direito e economia pela Universidade de Turim. Graduado em Direito pela Universidade Estadual de Maringá. Foi pesquisador visitante da The New School. Membro da Rede Latino-Americana de Vigilância, Tecnologia e Sociedade (Lavits) e do Instituto Brasileiro de Responsabilidade Civil (Iberc).

Em 2021, Danilo Doneda me disse que estávamos construindo algo muito bonito na Data Privacy Brasil. Em um seminário interno que organizamos para discutir a terceira edição do seu clássico livro Da Privacidade à Proteção de Dados Pessoais, Danilo disse que nossa força estava em manter um espírito universitário dentro de uma organização privada. Ou seja, a Data Privacy Brasil fazia ensino, pesquisa e extensão. Os pilares que organizam a universidade no Brasil.

O livro Entrelinhas: Explorando a Privacidade e Proteção de Dados em Comunidade carrega a marca desse espírito de pesquisa, ensino e extensão que caracteriza o trabalho da Data Privacy Brasil.

Diz respeito ao ensino, pois os autores deste livro fazem parte da comunidade de estudantes da escola da Data Privacy Brasil. Diz respeito à pesquisa, pois os diversos temas apresentados aqui são temas de fronteira no campo da pesquisa científica, como os debates sobre regulação do reconhecimento facial, avaliação de impacto algorítmico, compartilhamento de dados pessoais de saúde, entre outros. Também diz respeito à extensão, pois a iniciativa de reunir esses textos vêm de uma iniciativa da área de Comunidades e Novos Negócios da Data Privacy Brasil, responsável pelo Clube Data e pelos encontros chamados de “Data Talks”.

É importante a retomada da extensão no sentido dado por Paulo Freire. Não estamos falando de “assistência” a uma comunidade específica (a “extensão

assistencialista"), mas sim de construção de comunidades e de conhecimento por uma relação democrática e de libertação. Isso tem a ver com uma concepção sobre educação que também é freireana, que defendemos profundamente.

A educação é uma relação entre sujeitos. Ela é mediatizada por objetos que são cognoscíveis, no qual o educador também reconstrói seu ato de conhecer. Quando fazemos encontros como os do Clube Data, ou promovemos encontros de ensino-aprendizado com nossos estudantes, estamos a todo momento "problematizando o conteúdo que mediatiza os sujeitos", como diria Paulo Freire.

Essa problematização não é um "entretenimento intelectualista", como diria Freire, mas sim um ato que busca conexão com as situações concretas e reflexões que nos permitam agir melhor sobre o mundo social do qual fazemos parte.

Ao discutirmos os textos da comunidade de alunos e alunas da Data Privacy Brasil, nos permitimos, professores, um ato de reflexão, problematização e "dialeticidade" com a comunidade com a qual interagimos e buscamos criar laços significativos. É, também, uma oportunidade de uma "conscientização" para que possamos enxergar, coletivamente, problemas concretos de proteção de dados pessoais no Brasil e que transformações são necessárias para um adequado equilíbrio entre desenvolvimento econômico e tecnológico e respeito a direitos na sociedade da informação.

Por isso a ênfase, neste livro, de uma exploração em comunidade, que capta tão bem o espírito dos projetos liderados por Pedro Bastos, Gedeão França, Pedro Henrique Santos e toda a equipe dedicada à construção de comunidades na Data Privacy Brasil.

Uma cultura de direitos é feita no dia-a-dia, por cidadãos e profissionais. Estimular um debate por quem está na linha de frente de muitas das questões de aplicabilidade da Lei Geral de Proteção de Dados Pessoais, como é o espírito deste livro, é uma forma de fortalecer uma cultura forte de proteção de dados pessoais, reforçando o caráter comunitário de projetos com o Clube Data.

Espero que a leitura seja problematizadora e exponha esse caráter dialógico que tanto acreditamos quando pensamos em ensino-aprendizagem. Afinal, como disse Paulo Freire, "o conhecimento não se estende do que se julga sabedor até aqueles que se julga não saberem". Ele se constitui nas relações.

SEÇÃO I

Cultura de Privacidade & Design

Como e por que difundir a cultura de Privacidade e Proteção de Dados

Daiane Conde

1 introdução

Quando tratamos de privacidade e proteção de dados pessoais, é comum associarmos a conformidade aos avanços tecnológicos, como banners de cookies e criptografia. No entanto, o caminho para difundir o cuidado com os dados pessoais não deve se limitar a medidas tecnológicas. É fundamental que a cultura de privacidade esteja enraizada em todos os aspectos, e isso requer o engajamento e a conscientização das pessoas. Este artigo explora a importância da participação ativa de todos na salvaguarda das informações pessoais, tanto dentro como fora das organizações.

2 determinação legal

Embora a legislação nacional não possua um artigo específico dedicado à difusão cultura de privacidade, os princípios gerais já estabelecidos na Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018)[1], como os da boa-fé e da prevenção, destacam a importância de se promover a conscientização e garantir que todos os envolvidos no tratamento de dados estejam cientes de suas obrigações e responsabilidades.

Na mesma linha, a Autoridade Nacional de Proteção de Dados (ANPD) estabeleceu, no Regulamento de Dosimetria e Aplicação de Sanções Administrati-

vas[2] alguns fatores a serem analisados no momento da aplicação das sanções por essa autarquia. Para fins de análise do tema desse artigo, destacamos três deles:

> Art. 7º Na definição da sanção, devem ser considerados os seguintes parâmetros e critérios:
> II - a **boa-fé do infrator**;
> IX - a adoção reiterada e demonstrada de **mecanismos e procedimentos internos capazes de minimizar o dano**, voltados ao tratamento seguro e adequado de dados, em consonância com a LGPD;
> X - **a adoção de política de boas práticas e governança**;

Como se vê, a partir desse posicionamento da Autoridade Nacional de Proteção de Dados, a adoção de medidas que visem a propagar os conhecimentos acerca da privacidade e da proteção dos dados pessoais, podem ser utilizados como demonstrativos de cumprimento de critérios positivos em um momento crítico como o da aplicação das sanções, ganhando um peso ainda maior dentro do dia a dia dos agentes de tratamento.

3 **aplicação**

Embora cada agente de tratamento de dados possua características específicas, algumas medidas práticas comuns podem ser adotadas para promover a cultura de privacidade:

3.1 **treinamento no *onboarding***

No processo de integração de novos colaboradores, é importante disponibilizar materiais breves que expliquem conceitos básicos, como o que é a LGPD, definições de dados pessoais/dados pessoais sensíveis e a importância de protegê-los. Além disso, fornecer links para documentos mais detalhados, como um Aviso de Privacidade para Colaborador, e um endereço de contato para esclarecimento de dúvidas, ajuda a criar uma cultura de conscientização desde o princípio.

3.2 **treinamento da liderança**

Envolver a liderança é crucial, uma vez que eles desempenham um papel fundamental na definição de expectativas, tomada de decisões e transmissão de conhecimento. Realizar reuniões específicas e breves com os líderes pode incluir a conscientização sobre a importância de proteger dados pessoais e envolver a equipe de privacidade sempre que projetos ou processos envolverem essas informações.

Complementarmente, destacar o impacto positivo financeiro que a proteção de dados pode trazer pode ser um incentivo[3].

3.3 **privacidade no dia a dia**

A fim de superar a barreira técnica que muitas vezes afasta as pessoas ao ouvirem sobre LGPD e temas correlatos, é essencial conectar a legislação às atividades cotidianas das equipes. Os treinamentos podem ser adaptados de acordo com o público, destacando princípios relevantes para cada área, como a classificação entre controlador e operador para o setor jurídico e princípios como o da necessidade para o setor de recrutamento. Em resumo, a estrutura pode variar, mas o foco deve ser sempre o mesmo: relacionar as práticas cotidianas às diretrizes da LGPD.

Consequentemente, essas ações podem identificar pessoas mais engajadas durante os treinamentos, que podem ser recrutadas para programas específicos, como os "*privacy champions*", onde colaboradores de outras áreas atuam como defensores do tema.

3.4 **fora dos muros**

Além das orientações internas, é importante propagar a cultura de proteção de dados para o público externo. Isso demonstra boa-fé às autoridades de fiscalização, cria um diferencial de mercado[4] e melhora a comunicação com os titulares de dados, evitando conclusões equivocadas, como a ideia de que a LGPD proíbe o uso de dados.

Essa divulgação pode ser realizada de diversas maneiras, como por meio de posts em redes sociais ou comerciais mais elaborados, mas o foco deve ser

sempre o de envolver o público na disseminação do conhecimento.

4 **conclusão**

Promover a cultura de privacidade e proteção de dados gera benefícios significativos, como conformidade legal, fortalecimento da confiança, redução de riscos de segurança, melhoria na gestão de dados e estímulo à inovação responsável. É fundamental que a conscientização e o compromisso com a proteção de dados acompanhem o avanço tecnológico, garantindo a conformidade em uma era voltada a dados cada vez mais complexa e plural.

referências bibliográficas

BRASIL. **LEI Nº 13.709, DE 14 DE AGOSTO DE 2018**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 10 out. 2023.

BRASIL. **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. Acesso em: 01 out. 2023.

CONVERGÊNCIA DIGITAL. **Privacidade rende três vezes o investimento no Brasil**. Disponível em: https://www.convergenciadigital.com.br/Negocios/Privacidade-rende-tres-vezes-o-investimento-no-Brasil-62482.html?UserActiveTemplate=mobile&amp. Acesso em: 18 out. 2023.

G1 . **Privacidade: 77% dos brasileiros já desinstalaram apps por preocupação com dados pessoais, diz pesquisa**. Disponível em: https://g1.globo.com/tecnologia/noticia/2022/08/18/brasileiros-apps-dados-pessoais-redes-sociais.ghtml. Acesso em: 9 out. 2023.

LEAL, Martha. **Apple e Facebook: a privacidade como ativo de mercado**. Monitor Mercantil, 9 jun. 2023. Disponível em: https://monitormercantil.com.br/apple-e-facebook-a-privacidade-como-ativo-de-mercado/. Acesso em: 18 out. 2023.

YOUTUBE. **Privacidade no Iphone**. Disponível em: https://www.youtube.com/watch?v=AJu8xUBzbLQ&ab_channel=AppleBrasil. Acesso em: 10 out. 2023.

notas de rodapé

1 BRASIL. **LEI Nº 13.709, DE 14 DE AGOSTO DE 2018**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 10 out. 2023.

2 BRASIL. **LEI Nº 13.709, DE 14 DE AGOSTO DE 2018**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 10 out. 2023.

3 Privacidade rende três vezes o investimento no Brasil. **Convergência Digital**. São Paulo, 08 fev. 2023. Disponível em: https://www.convergenciadigital.com.br/Negocios/Privacidade-rende-tres-vezes-o-investimento-no-Brasil-62482.html?UserActiveTemplate=mobile&amp. Acesso em: 18 out de 2023.

4 LEAL, Martha. **Apple e Facebook**: a privacidade como ativo de mercado. São Paulo, Monitor Mercantil, 9 jun. 2023. Disponível em: https://monitormercantil.com.br/apple-e-facebook-a-privacidade-como-ativo-de-mercado/. Acesso em: 18 out. 2023.

Privacy by Design

Julie Borges

1 introdução

No mundo contemporâneo, frequentemente descrito como a "era dos dados", a crescente onipresença da tecnologia resultou em uma acumulação sem precedentes de dados. Por isso, a privacidade e a proteção emergem como questões críticas, exigindo uma reavaliação contínua das práticas e políticas.

Pensando nisso, a necessidade de uma abordagem proativa e essencial para enfrentar esses desafios, por meio de metodologias de design, gerou o conceito de "Privacy by Design" (PbD).

Este artigo visa disseminar como funciona e deve ser implementado o PbD, perpassando por seus conceitos, os 7 princípios norteadores, além de um giro sobre a atual regulamentação ao redor do mundo..

1.1 o que é design?

Para fins de entendimento, é necessário iniciar a elaboração deste artigo com alguns conceitos importantes que não possuem natureza jurídica ou digital, como Design. Objetivamente, design é sobre resolver problemas. Para isso, ele possui muitos ramos diferentes definidos pelo tipo de desafio que o designer está tentando resolver.

O design apresenta técnicas e prioridades voltadas para a transformação do setor aplicado, neste caso, o jurídico. Assim, é possível alinhar os resultados legais com as expectativas de seus usuários e

desenvolver visões inovadoras e ambiciosas para a oferta de serviços.

De modo geral, o design tem como foco as pessoas e seus contextos específicos, analisa como a situação atual pode ser aprimorada e explora o uso da tecnologia como uma forma de intervenção[1].

Margareth Hagan entende que: "design é sobre criar coisas que são intuitivas, envolventes, valiosas e queridas pelas pessoas que as utilizam.[2]" Sendo assim, quando aplicamos o design nos deparamos uma mudança na forma pensar a privacidade, melhorando suas funcionalidades e usabilidade.

O erro mais comum dos não-designers em relação ao design é pensar que se trata apenas de embelezar, afiar ou melhorar a estética de algo. Ainda que a aparência seja um aspecto crucial no design de um objeto, ela não representa a totalidade de suas contribuições e, definitivamente, não é a essência do que realmente significa.

2 **privacy by design**

No campo da Privacidade e Proteção de Dados - PPD, a aplicação do Design cria um novo conceito: Privacy by Design (PbD). Também considerado como um tipo de "tecnologias de aprimoramento da privacidade" (do inglês: "*Privacy-Enhancing Technologies - PET*"[3]).

Popularizado em 2009, o conceito de PbD foi desenvolvido pela ex-Comissária de Informações e Proteção de Dados de Ontário, Canadá, Ann Cavoukian, na 31ª Conferência Internacional de Proteção de Dados e Comissários de Privacidade que Cavoukian quando apresentou o workshop "Privacy by Design: The Definitive Workshop" na década 1990[4].

No ano seguinte, o PbD alcançou o status de padrão internacional com a aprovação unânime da "Resolução sobre Privacy by Design" durante a 32ª Conferência Internacional de Proteção de Dados e Comissários de Privacidade.

A conferência reconheceu o PbD como um elemento fundamental para a proteção da privacidade. Desde então, o PbD tem sido adotado globalmente por formuladores de políticas públicas como uma norma regulatória para a governança de dados e privacidade[5].

De maneira resumida, a aplicação do Design aos programas de Privacidade e Proteção de Dados é feita por meio de uma metodologia com 7 princípios que tem como objetivo central desenvolver algo nos moldes de ideais de privacidade. São eles: Proativo e não reativo, preventivo e não corretivo; Privacida-

de como configuração padrão (*Privacy by Default*); Privacidade Incorporada ao Design; Funcionalidade Completa; Segurança em todo o ciclo de vida do dado; Visibilidade e transparência; e Foco no usuário.

Seguindo esses princípios, será possível desenvolver um produto ou serviço em que os mais altos padrões de privacidade integram a matriz de desenvolvimento, fazendo um caminho reverso ao que hoje vemos acontecendo. Atualmente, a privacidade é coadjuvante na maioria dos processos de criação e desenvolvimento, ainda que deva ser o motor central de muitas operações e negócios.

2.1 os princípios do privacy by design (PbD)

À medida que navegamos na complexa interseção entre tecnologia e privacidade, a abordagem do Privacy by Design emerge como um farol orientador, propondo uma fusão harmoniosa entre proteção de dados e inovação tecnológica.

Isso não acontece de forma desordenada e a metodologia composta por 7 princípios concretiza-se de forma ordenada e intencional, como tudo do Design.

Nesse cenário, cada princípio reflete uma compreensão profunda das necessidades e desafios inerentes à Proteção de Dados na era digital e juntos, formam um conjunto robusto de diretrizes que não apenas salvaguardar a privacidade do usuário, mas também incentivam um design inovador e responsável. são eles:

a. **Proatividade, Não Reatividade; Prevenção, Não Remediação:** devemos antecipar e prevenir eventos invasivos à privacidade antes que aconteçam, não esperando os riscos de privacidade se materializarem, nem oferecendo remédios para infrações de privacidade após ocorrerem – seu objetivo é preveni-las.

b. **Privacidade como Configuração Padrão (*Privacy by Default*):** todos os dados pessoais devem ser protegidos no modo de configuração básica do sistema, ou seja, se o indivíduo não alterar nenhuma configuração, sua privacidade permanece intacta. A privacidade é incorporada ao sistema como configuração padrão.

c. **Privacidade Incorporada ao Design:** a privacidade deve estar integrada ao design e à arquitetura do sistemas e as práticas do negócio, não sendo um

adicional posterior. Isso faz com que a privacidade seja uma parte essencial da funcionalidade principal oferecida, sem diminuir a funcionalidade.

d. **Funcionalidade Completa – Ganha-Ganha, Não Zero-Soma:** o objetivo é acomodar todos os interesses e objetivos legítimos de maneira "ganha-ganha", evitando perdas de funcionalidade desnecessárias e falsas dicotomias, como privacidade versus segurança, mostrando que é possível ter ambos[6].

e. **Segurança de Ponta a Ponta – Proteção Completa do Ciclo de Vida:** quando incorporado ao sistema desde o início, o PbD estende a segurança por todo o ciclo de vida dos dados envolvidos, garantindo que todos os dados sejam retidos de forma segura e, em seguida, destruídos de forma segura e oportuna no final do processo.

f. **Visibilidade e Transparência – Manter Aberto:** no processo, todas as partes interessadas que, independentemente da prática empresarial ou tecnologia envolvida, operam de acordo com as promessas e objetivos declarados, sujeitos à verificação independente. Por isso, as operações permanecem visíveis e transparentes, tanto para usuários quanto para provedores.

g. **Centrado no Usuário:** Acima de tudo, o PbD exige que arquitetos e operadores mantenham os interesses do indivíduo em primeiro lugar, oferecendo medidas como fortes configurações padrão de privacidade, notificações apropriadas e opções amigáveis e empoderadoras para o usuário.

2.2 **privacy by design nas legislações**

Somente com a implementação do Regulamento Geral sobre a Proteção de Dados (GDPR) na União Europeia em 2018[7] as abordagens de *Privacy by Design* e *by Default* tornaram-se um requisito legal conforme estabelecido no Artigo 25[8].

No documento de 2018, formulou-se um conceito mais amplo de medidas de privacidade desenvolvido em discussões internacionais ao longo dos anos, enquanto as Guidelines 4/2019 apontam especificamente as obrigações legais do GDPR.

No Brasil, a Lei Geral de Proteção de Dados (LGPD) segue a inspiração da legislação europeia. Embora não mencione explicitamente o Privacy by Design, os princípios da lei refletem sua filosofia, especialmente no Artigo 46 e seu § 2°, que enfatizam a importância de medidas de segurança desde a concepção do produto ou serviço. Esta inclusão na LGPD visa assegurar que a proteção de dados seja integrada desde o início do desenvolvimento, cumprindo com os padrões legais estabelecidos[9].

3 **conclusão**

Ao longo deste artigo, exploramos o status e a metodologia do *Privacy by Design*, especialmente no contexto da GDPR e da LGPD. Além disso, entendemos que o PbD transcende a mera conformidade legal, incorporando uma abordagem ética e proativa à privacidade e proteção de dados, refletindo não apenas uma necessidade regulatória, mas um compromisso com os direitos fundamentais dos indivíduos.

Em um mundo cada vez mais orientado por dados, o PbD não é apenas um método para cumprir com regulamentos, mas um compromisso ético para com a proteção da privacidade dos indivíduos, tornando-se um passo crucial para construir uma sociedade digital mais segura e confiável.

À medida que avançamos na era digital, é imperativo que organizações, legisladores e profissionais da tecnologia continuem a adotar e refinar esses princípios, assegurando que a privacidade e a proteção de dados sejam consideradas como elementos fundamentais e não como meros requisitos regulatórios.

notas de rodapé

1 HAGAN, Margareth. **Law by Design**. Disponível em: https://lawbydesign.co/legal-design/. Acesso em: 09 nov. 2023.

2 HAGAN, Margareth. **Law by Design**. Disponível em: https://lawbydesign.co/legal-design/. Acesso em: 09 nov. 2023.

3 Tradução Livre.

4 HUSTINX, Peter. **Privacy by Design**: Delivering the Promises, Madrid, 2009.

5 BENTES, Anna... [*et al.*]. **Para além da proteção de dados [livro eletrônico]:** uma coletânea. São Paulo: Data Privacy Brasil Ensino, 2023.

6 CAVOUKIAN, Ann. **Privacy by design**. The seven foundational principles. Implementation and mapping of fair information practices, 2010.

7 European Data Protection Supervisor. **Opinion 5/2018**. Preliminary Opinion on privacy by design, 2018.

8 European Data Protection Board. **Guidelines 4/2019** on Article 25 Data Protection by Design and by Default, 2019.

9 BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 2a ed. Rio de Janeiro: Forense, 2021.

SEÇÃO II

Aplicação da LGPD em Contextos Específicos

Dados de saúde e as bases legais para tutela da saúde tendo o paciente com a centralidade da proteção dos dados pessoais

Bárbara Steffens

1 o direito fundamental à proteção de dados, a lei 13.709/2018 e a tutela da saúde

Muito embora estejamos imersos no universo digital, a proteção e a privacidade de dados pessoais no Brasil enfrentaram muitos desafios até a edição do mais relevante marco regulatório: a Lei Geral de Proteção de Dados (LGPD, Lei nº. 13.709/2018).

Inegável que a lei brasileira foi inspirada e sofreu significativa influência da pioneira regulação da União Europeia, que elaborou o Regulamento Geral sobre Proteção de Dados (GDPR).

A lei surgiu da necessidade de se proteger a privacidade em razão das mudanças tecnológicas que, apesar de trazem inúmeros benefícios, também representam ameaça ao espaço individual pois por meio das informações é possível que se conheçam, por exemplo, os padrões de compra, o time de futebol do coração, as preferências políticas, entre outras. O cruzamento dessas informações pode prejudicar as pessoas, expor situações privadas, fornecer informações que muitas vezes as pessoas não querem divulgar.

No Brasil, o direito à proteção de dados estava implícito no direito à privacidade e intimidade previstos na Constituição Federal, alcançando status constitucio-

nal somente após a aprovação da Emenda Constitucional 115/2022, a qual acresceu ao artigo 5º, o inciso LXXIV, robustecendo, assim, a legislação infraconstitucional.

Desse modo, a análise busca esclarecer qual a base legal para o tratamento dos dados da saúde em consonância com os princípios da Lei Geral de Proteção de Dados, no contexto das práticas de exames laboratoriais, que envolvem o titular dos dados pessoais, o controlador e o operador, e a inafastabilidade do compartilhamento dos dados nos casos em que a tutela da saúde mostra-se como principal critério na ponderação entre o direito à proteção dos dados no âmbito da privacidade e intimidade e a efetividade do tratamento médico necessário para a manutenção da saúde.

2 os dados (sensíveis) da saúde e a(s) base(s) legal para o tratamento especialmente no âmbito dos laboratórios de análises clínicas

Os dados da saúde são considerados dados pessoais sensíveis, isto é, em razão da sua natureza recebem da lei tratamento ainda mais rigoroso porque o desvirtuamento do tratamento gera graves consequências, inclusive discriminatórias, que foge totalmente ao escopo da LGPD.

Essa classificação é suficiente para embasar o entendimento de que todos os dados contidos em prontuários médicos, receitas, guias de internações, guias de solicitação de exames e os respectivos resultados, laudos, etc., integram o conjunto de dados sensíveis.

A relação entre os profissionais da saúde e seus pacientes, leia-se titular dos dados, é de grande confiança, e o conhecimento do histórico de saúde como realização de tratamentos, utilização de medicamentos, resultados de exames já realizados e o diagnóstico de outros profissionais, são pressupostos para a coleta de informações que embasem o melhor tratamento possível para a conservação da saúde do paciente.

Dessa forma, a base legal do consentimento não é a adequada, pois o tratamento da saúde no sentido de manutenção e preservação da qualidade de vida, prepondera sobre o interesse pessoal do titular. No entanto, o consentimento poderá preponderar em casos, por exemplo, de intervenções de baixo risco ou de natureza estética e, ainda, quando o compartilhamento se der com terceiro que não trata os dados em virtude da tutela da saúde.

Dado o vasto campo sanitário, a presente abordagem centra-se no trata-

mento de dados pessoais realizado por laboratórios de análises clínicas, que não foge à regra de que o manuseio destes dados pessoais deve ser realizado por profissionais da saúde, serviços de saúde e autoridades sanitárias para que a base legal esteja legitimada[1].

No caso central objeto do presente artigo, a coleta das amostras e seu encaminhamento para o setor responsável pela análise clínica; emissão de laudo diagnóstico; divulgação do resultado para o paciente; armazenamento dos resultados, quando realizados por profissional de saúde obrigado ao sigilo médico, a base legal aplicável é a tutela da saúde. Observe-se que as diferentes etapas na prestação de serviços laboratoriais constituem-se em verdadeira teia de relacionamentos, multiplicando a responsabilidade dos agentes de tratamento de dados e seus colaboradores, aumentando os cuidados a serem implementados.

Partindo-se desta premissa, passa-se à análise dos agentes de tratamento. A coleta primária dos dados com o objetivo de utilizá-los para a prestação de serviços, torna o laboratório de análises clínicas o controlador dos dados pessoais, pois uma vez que o paciente solicita os seus serviços, claro que munido da respectiva solicitação pelo médico, ele é o agente que possui o *know how* para a correta prestação de serviço, determinando as etapas do atendimento para que o resultado final, os exames, seja alcançado de modo a subsidiar o tratamento médico a ser aplicado.

Entretanto, caso o laboratório preste serviços a um hospital, será então o operador dos dados, uma vez que a instituição é quem tomará as decisões quanto ao tratamento dos dados da saúde, respondendo o hospital pelos seus colaboradores e corpo clínico, e o laboratório igualmente, no âmbito de sua organização interna.

É de se ressaltar, ainda, o papel imprescindível dos laboratórios de apoio, responsáveis por análise clínica específica, cuja prestação de serviço não pode ser contemplada pelo controlador, e que se revela imprescindível nesta cadeia de tratamento da saúde envolvendo o paciente. O laboratório de apoio, por sua vez, deverá observar rigorosamente as normas éticas e regulatórias do setor, e as disposições da LGPD, respondendo pelos cuidados que lhe competem segundo a legislação. Acrescente-se o fato de que o laboratório controlador dos dados tem o direito de exercer o seu poder fiscalizatório quanto ao *compliance* de todos os agentes envolvidos, seja pela requisição de documentos, seja por meio de auditorias.

Nesse mesmo norte, os laboratórios compartilham os dados com as operadoras de planos de saúde e com o sistema público, com o objetivo de atender às finalidades específicas.

Ainda que a base legal de proteção da saúde seja aplicada primordialmente, é seguro informar ao titular o compartilhamento dos dados, seja por meio do contrato assinado com o hospital, clínica e o próprio laboratório, informando ao titular dos dados a outra parte que acessará seus dados e quais os dados estarão disponíveis, seguindo-se o princípio da finalidade do compartilhamento. (COSTA; MONACO, 2021, p. 98)

Em um primeiro momento, poder-se-ia concluir que o consentimento integra o compartilhamento de dados no sentido de atender aos requisitos previstos no artigo 5º, inciso XII, da lei 13.709/2018, de modo a ser oportunizada uma escolha real ao titular dissociada de termos e condições. Por outro lado, é sabido que a qualquer momento o consentimento pode ser revogado, ocupando, assim fator de alto risco, podendo influenciar decisivamente na aplicação do tratamento determinado pelo profissional da saúde.

Utilizando-se o consentimento, é premente, portanto, que se busque uma alternativa para que o serviço não comprometa a tutela da saúde do paciente. Neste caso, ao titular dos dados deverá ser esclarecido de forma objetiva e acessível, que o compartilhamento é imprescindível para uma avaliação mais precisa de seu quadro de saúde. Só assim, munido destas informações, seu consentimento será válido, porque qualificado pela manifestação livre e inequívoca.

Por outro lado, o inciso II do artigo 11 dispensa o consentimento em caso de dados sensíveis para a tutela da saúde, porém não tece o legislador maiores considerações. Assim, pode-se encontrar melhor suporte no Regulamento Europeu (GDPR):

> [...] sugere-se a utilização do conceito previsto na legislação europeia, aplicando-se a tutela da saúde apenas se o tratamento for necessário para efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistemas e serviços de saúde ou de ação social, se os dados forem tratados por ou sob a responsabilidade de um profissional sujeito à obrigação de sigilo profissional. (BRASIL, 2021, p. 75)

A classificação da posição de agente de tratamento é relevante para fins de apuração de responsabilidades em caso de violação de dados, que poderão re-

dundar em processo administrativo fiscalizatório pela Autoridade Nacional de Proteção de Dados (ANPD), ou ações judiciais. Nestes casos, o agente é quem deverá defender a sua própria posição a partir da finalidade específica do tratamento de dados e o papel de cada envolvido na cadeia de tratamento, tendo em vista o caso concreto.

Desse modo, a gestão de terceiros é importante, pois tanto controlador e operador têm obrigação de reparação em caso de dano. Por isso, a segurança jurídica em caso de compartilhamento dos dados serve como suporte para que as relações comerciais sejam realizadas de forma mais robusta. Logo, não se trata apenas da subsunção da norma ao caso concreto, para além disso, a LGPD influencia as relações sociais, comerciais, trabalhistas, por exemplo.

As empresas ligadas ao setor da saúde estão entre as mais visadas pelos ataques cibernéticos, já que os criminosos têm perfeita dimensão do quanto ataques dessa natureza podem ser prejudiciais, e até inviabilizar os atendimentos médicos, elevando consideravelmente os valores exigidos para o restabelecimento do sistema operacional interno. Caso a organização não contenha medidas de segurança eficientes, tais como backup atualizado, métodos de garantia da confidencialidade e integridade dos bancos de dados, o abalo de sua imagem perante os clientes/pacientes, e a continuidade segura dos serviços, resultam em forte abalo econômico para além da violação de direitos fundamentais.

Ainda relativamente ao consentimento o paciente, enfatiza Walkiria Favero (2012, p. 186)

> Por fim, importante frisar que o respeito à **finalidade** (o tratamento de dados deverá ser pautado em um objetivo claro), que tem de ser no interesse da saúde do paciente do tratamento dos dados pessoais de saúde, de acordo com a **necessidade** (apenas poderão ser coletados os dados pessoais estritamente necessários para o objetivo determinado) e da **transparência** (o objetivo determinado deverá ser transparente ao titular destas informações) são a resposta para a conciliação entre os direitos fundamentais da privacidade da saúde. Se a tutela da saúde permite que dados pessoais de saúde sejam tratados mesmo sem o consentimento dos titulares, o cuidado na manutenção da finalidade original é a garantia de que haja de fato excepcionalidade no tratamento. (FAVERO, 2012, p. 186)

Pela via do exposto, a base legal para o tratamento dos dados em face de tutela da saúde é suficientemente legítima para afastar o consentimento o paciente, desde que o tratamento dos dados seja com a finalidade exclusiva de iniciar o tratamento da saúde, ou continuidade do mesmo, sob o controle de profissionais da saúde (médicos, enfermeiros, educadores físicos, nutricionistas, fisioterapeutas, etc.), serviços de saúde e autoridades sanitárias.

No caso de tratamento destes dados sensíveis por pessoa jurídica fora da área da saúde, o consentimento torna-se, obrigatoriamente, a base legal para o compartilhamento dos dados.

3 **considerações finais**

A vulnerabilidade do titular de dados/paciente impele o reconhecimento de seus direitos, fundamentados na proteção da sua dignidade, promovendo a sua autonomia e a prevenção dos danos decorrentes dos cuidados com a saúde.

Sendo assim, a proteção dos direitos do paciente vão além dos princípios do Direito Médico (e sua regulamentação), há que se alicerçar no ecossistema de proteção da pessoa, justificando-se, assim, a utilização da base legal para o respectivo tratamento, a tutela da saúde realizada por profissional desta área, e, havendo a necessidade de compartilhamento dos dados com terceiros, embora se exija a tomada do consentimento, também há de se considerar que este terceiro participa da cadeia de tratamento contribuindo para a continuidade e efetividade do tratamento, sendo imprescindível a sua colaboração de modo a fornecer o mais completo possível o número de informações que possam preservar a sua saúde ou restabelecê-la.

Logo, no ecossistema da saúde, a centralidade é da pessoa mais especialmente no sentido de que a confidencialidade do paciente seja protegida ainda mais pela a interpretação sistemática da LGPD quanto à tutela da saúde, que deve ser pautada pelo respeito ao paciente, enquanto titular de dados pessoais e sujeito ativo do cuidado com a sua saúde.

referências bibliográficas

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado**. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf. Acesso em: 5 nov.2023.

BRASIL. **Confederação Nacional da Saúde**. Código de boas práticas: proteção de dados para prestadores privados em saúde. MENDES, Laura Schertel, *et al*. Brasília. 2021.

BRASIL. **Lei 13.709, de 14 de agosto de 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 12 nov. 2023.

COSTA, José Augusto Fontoura. **Tratamento e transferência de dados de saúde: limites e responsabilidade de dados sensíveis**. DALLARI, Analuza Bolivar; MONACO, Gustavo Ferraz de Campos (Coord.). LGPD na saúde. São Paulo: Thompson Reuters Brasil, 2021, p. 89-102.

FAVERO, Walkiria Nakano Eloy. **Proteção e compartilhamento de dados na saúde suplementar**. DALLARI, Analuza Bolivar; MONACO, Gustavo Ferraz de Campos (Coord.). LGPD na saúde. São Paulo: Thompson Reuters Brasil, 2021, p. 171-194.

notas de rodapé

1 A regularidade formal do exercício de atividade no campo da saúde se dá com a normatização de cada profissão.

A Lei Geral de Proteção de Dados Pessoais no Contexto das Escolas Particulares

Luciano Escobar

1 introdução

Há mais de dez anos tenho me especializado em Direito Educacional e prestado consultoria jurídica preventiva, inclusive desenvolvendo projetos de adequação à LGPD, para instituições de ensino privadas no segmento da educação básica. Assim sendo, este artigo é a expressão escrita e com maior aprofundamento da apresentação e debates realizados no 4º *Data Talks, promovido pela Data Privacy Brasil*[1], com novas reflexões ancoradas pela articulação da teoria com a prática jurídica.

Já de início, trago um depoimento a respeito dos cursos da Data Privacy que foram essenciais na minha formação, tanto por seus conteúdos extremamente sólidos e aprofundados, quanto, principalmente, pela sua preocupação com desenvolvimento humano, deixando claro que, para se poder assegurar o aprimoramento livre dos indivíduos, é preciso garantir a proteção dos dados e informações a seu respeito e que hoje têm uma posição de subjetividade, porque incorporados à sua personalidade, ou seja, correspondem a atributos próprios e únicos que o definem como pessoa humana, mas que não o diferem de qualquer outra, porque ambas, independentemente de seus atributos próprios, são sujeitos dos mesmos direitos.

Essa me parece ser a essência da *Data Privacy,* dotar as pessoas com o conhecimento e entendimento necessário para que haja a transformação da sociedade para a efetivação do livre desenvolvimento da sua personalidade humana, trazendo a definição de autodeterminação informativa para o ambiente da realidade prática[2].

Dessa maneira, este artigo aborda a aplicação da Lei Geral de Proteção de Dados (LGPD) no contexto das escolas particulares de educação básica[3], destacando a importância da proteção da privacidade, particularmente da criança e do adolescente, no ambiente educacional e a constante necessidade de tratamento de dados pessoais pelas escolas para avaliar a eficiência da sua prática pedagógica e o resultado no processo de ensino e aprendizagem. Como metodologia, adotamos a observação empírica e a revisão bibliográfica. A premissa é a de que a educação brasileira está cada vez mais centrada na análise de dados e no perfilamento dos estudantes, tornando crucial a aplicação correta da proteção de dados no ambiente escolar. Por isso, este texto enfatiza a necessidade da efetivação da LGPD como cumprimento de obrigação legal e regulatória, conectando-a aos direitos fundamentais à educação e ao livre desenvolvimento pleno da pessoa. Além disso, destaca-se a importância de integrar a Lei ao projeto político-pedagógico da escola, promovendo uma mudança cultural e educacional. Também são abordadas as crescentes preocupações relacionadas ao tratamento de dados pessoais no ambiente educacional, especialmente com a presença cada vez maior de tecnologia proporcionado pelo crescente surgimento das *EdTechs*.

A literatura especializada, exemplificada pela obra de Cathy O'Neil (2020)[4], revela que tais informações são frequentemente empregadas para alimentar algoritmos que classificam e hierarquizam os estudantes de maior destaque, muitas vezes em um processo opaco e carente de transparência no contexto das decisões automatizadas. Em virtude dessa conjuntura, torna-se fundamental implementar medidas de salvaguarda que visem garantir a privacidade e a segurança dos dados pessoais dos educandos, afastando qualquer prática discriminatória e assegurando a conformidade com os princípios éticos, jurídicos e pedagógicos pertinentes. A proteção de tais dados deve ser abordada de forma holística e responsável, considerando os impactos futuros e a imperativa necessidade de uma regulamentação adequada a fim de preservar os direitos fundamentais à privacidade e à igualdade de oportunidades dos discentes em um contexto pós-formativo.

O presente texto, sobre a Lei Geral de Proteção de Dados no Contexto das

Escolas Particulares de Educação Básica tem por princípio apresentar de uma forma breve e leve o tema, procurando despertar a curiosidade e o futuro aprofundamento, quanto aos contextos dos tratamentos de dados pessoais ocorrentes no ambiente escolar de crianças e adolescentes, portanto, hiper vulneráveis.

2 **desenvolvimento**

É da natureza de toda e qualquer instituição de ensino, para a realização da sua atividade fim e de sua prática pedagógica, na consecução do processo de ensino e aprendizagem de seus alunos, a ocorrência de diversas operações de tratamentos de dados pessoais, praticamente, de forma constante.

Não é possível para a escola saber o quão eficiente é a sua metodologia de ensino se não houver uma forma de avaliar a aprendizagem e o desenvolvimento dos seus alunos, ou até mesmo medi-la (mais quantitativa do que qualitativamente), através dos mais diversos processos avaliativos, para extrair os resultados que permitirão concluir eles o quanto conseguiram aprender e apreender referente aos conteúdos didáticos estabelecidos pela BNCC e pela LDB, para que, ao final de respectivo ano letivo, seja possível atestar sua aprovação ou reprovação. Isso evidencia o quanto a educação brasileira está centrada na análise de dados e perfilamento de seus estudantes.

A eficiência do processo de escolarização é essencial à sobrevivência das instituições de ensino, no caso, as particulares. Estas, em razão da alta competitividade, precisam manter os melhores índices de aprovação, de ingresso em universidades no Brasil e exterior, garantindo assim o crescimento de novas matrículas.

Toda a prática docente, e sua atividade pedagógica, é centrada no tratamento de dados pessoais dos alunos, objetivando, em última análise, medir a eficiência/eficácia do processo de escolarização de uma instituição de ensino através dos indicadores gerados. E, perceba-se, ao se analisar o desempenho de um estudante, através dos seus resultados avaliativos, está-se de forma transversa, analisando também a capacidade docente de ensinar. Por isso o motivo da importância e da essencialidade da correta aplicação da Lei Geral de Proteção de Dados no ambiente escolar.

2.1 **LGPD: a necessidade da efetivação como cumprimento de obrigação legal e regulatória**

A educação é direito fundamental a ser provido pelo Estado, nos termos dos artigos 205[5] e 227[6] da Constituição Federal e nos artigos 53[7] e 54[8] do Estatuto da Criança e do Adolescente (ECA) Lei n.º 8.069/90 e que encontrou regulamentação na Lei de Diretrizes e Bases da Educação, Lei n.º 9.394/96.

A educação, ou seja, o fazer docente, visa ao pleno desenvolvimento da pessoa, seu preparo para o exercício da cidadania e sua qualificação para o trabalho. Na sua essência, significa desenvolver em cada aluno a sua capacidade de exercer a sua autodeterminação informativa, o seu desenvolvimento seguro, como ser em formação, proporcionando a sua construção como cidadão, com a aquisição do pensamento crítico, através do acesso pleno ao conhecimento.

Daí porque o que de primeiro se deve ter presente, ao se pretender trazer a Lei Geral de Proteção de Dados para o âmbito da educação (seja básica ou superior) é de reconhecer a necessidade do seu alinhamento ao projeto político pedagógico da escola, de forma transversal ao longo de toda a formação tanto de alunos quanto de educadores. Antes de a lei ser vista como um instrumento regulatório, tendo a Escola como alvo de adequação, para a implementação de um ambiente de conformidade legal, ela precisa ser vista como mais um instrumento de escolarização e transformação social.

Importante ressaltar que, a incidência da LGPD em si, junto ao ambiente educacional encontra suporte legal na necessidade de cumprimento de obrigação legal ou regulatória.

Se há a pretensão de uma mudança de cultura e internalização no pensamento e conduta humana quanto ao reconhecimento de que dados pessoais são atributos de personalidade e que, portanto, precisam ser vistos e garantidos dessa forma pela própria sociedade, é necessário que isso seja trabalhado no contexto da escolarização e da educação escolar, entendida como aquela atividade própria das Escolas de ensinar para o pleno desenvolvimento do educando e seu preparo para o exercício da cidadania. E isto vai muito além de se estabelecer campanhas de conscientização e capacitação, nos moldes daqueles que são estabelecidos em projeto de adequação para a conformidade de uma organização à LGPD.

Tanto isso é verdade que, a própria BNCC[9], homologada em 2018, tratou de prever os eixos de Cultura Digital, Tecnologia Digital e Pensamento Computacional, que deveriam ser desenvolvidos na formação da educação básica, na

promoção da alfabetização e do letramento digital, conforme vem destacado na competência geral 5:

> "Compreender, utilizar e criar tecnologias digitais de informação e comunicação de forma crítica, significativa, reflexiva e ética nas diversas práticas sociais (incluindo as escolares) para se comunicar, acessar e disseminar informações, produzir conhecimentos, resolver problemas e exercer protagonismo e autoria na vida pessoal e coletiva." (BNCC, 2018)

Mas foi somente agora, em 2023, talvez impulsionada pela própria LGPD, que a houve a alteração do inciso XII e Parágrafo Único do art. 4º da LDB, através da uma Política Nacional da Educação Digital - PNED[10], que incluiu a educação digital e o letramento digital, no âmbito da educação básica[11].

Aliás, em sendo um dos principais fundamentos da LGPD, para a proteção de dados, os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (art. 2º, VII), há a necessidade de que os tratamentos de dados pessoais ocorram de forma justa e lícita, fazendo total sentido que isso se dê através da promoção da educação voltada para a realidade existencial das próprias crianças e adolescentes, que nascem imersas em um ambiente digital, altamente tecnológico. Isto é a percepção de ética e cidadania deve ser construída a partir de uma ética e cidadania para o ambiente digital.

Portanto, esse é o primeiro aspecto que se deve ter a respeito das instituições de ensino através do olhar da Lei Geral e Proteção de Dados.

Se observarmos os exemplos vindo do exterior, nas mais conceituadas e ativas Autoridade de Proteção de dados mais ativas, veremos que é exatamente esse o movimento, paralelo ao de enforcement da lei, inclusive com a produção de materiais para apoiar e auxiliar as escolas em como ensinar os alunos sobre a importância da proteção de dados pessoais, como é o caso:

a) **Reino Unido: ICO – *Information Commissioner's Office*[12]**, que produziu um conjunto de materiais para os professores usarem ao discutir questões de privacidade e o valor dos dados pessoais. Os planos de aula abordam o que são dados pessoais, por que são valiosos e como mantê-los seguros ao usar as redes sociais[13];

b) **França: CNIL** - ***Commission Nationale de l'Informatique et des Libertés***[14], realiza o concurso "Troféus de Classe" com o objetivo de desenvolver uma cultura ética no uso dos dados pessoais no ambiente digital. Isto inclui conhecer os direitos e deveres relacionados com a utilização da Internet, saber proteger a privacidade e os dados pessoais, para uma utilização responsável das ferramentas e recursos digitais online[15];

c) **Espanha: AEPD** - ***Agencia Española Protección Datos***[16], através da Conferência do Setor de Educação sobre certificação, credenciamento e reconhecimento da competência digital docente, estabeleceu que os professores receberão as competências digitais e a formação necessária para o ensino e transmissão de valores e direitos que garantam a plena inserção dos alunos na sociedade digital e a aprendizagem do consumo responsável e do uso crítico e seguro dos meios digitais que respeitem a dignidade humana, a justiça social e a sustentabilidade ambiental, os valores constitucionais e fundamentais[17];

d) **Irlanda: DPC – *Data Protection Commission***[18], que em maio de 2022 publicou três pequenos guias para crianças sobre os seus direitos de proteção de dados pessoais, intitulados: "Proteção de Dados – Do que se trata?", "Meus Direitos à Proteção de Dados"[19] e "Principais dicas para manter seus dados pessoais seguros online"[20];

2.2 a contextualização das escolas de ensino privado

A União edita normas gerais da estruturação da educação no Brasil, através da lei de diretrizes e bases da educação LDB – Lei n.º 9.394/96, a BNCC – Base Nacional Comum Curricular e as resoluções e pareceres do MEC, produzidos a partir da sua Câmara de educação básica.

Cabe aos Estados e ao Distrito Federal organizarem os seus sistemas de ensino, que englobam escolas públicas e particulares, cujos efeitos e aplicabilidade se dão sobre as escolas que mantenham ensino fundamental e médio. São os sistemas de ensino estadual e municipal que editam as regras de funcionamento de uma instituição de ensino no âmbito de suas competências. Assim, essa é uma primeira distinção importante que terá reflexos incidindo diretamente sobre tratamento dos dados pessoais da comunidade escolar.

A segunda distinção que se faz é exatamente quanto a existência de escolas públicas e particulares. O modelo e padrão realizados pelo legislador era o de somente escolas públicas e assim foi durante muitos anos. Veja-se que a Constituição de 1967 trazia no parágrafo primeiro do artigo 169, que o ensino seria ministrado, nos diferentes graus, pelos poderes públicos. No seu parágrafo segundo, respeitadas as disposições legais, o ensino seria livre à iniciativa particular, a qual mereceria o apoio técnico e financeiro dos poderes públicos, inclusive bolsas de estudos.

O que se pode afirmar é que até 1967, as escolas particulares ficaram renegadas a um segundo plano. É a partir da Constituição de 1988, que as escolas privadas tomam um corpo e um maior volume no processo de escolarização ou de ensino-aprendizagem por conta da forma bastante deficitária, das escolas públicas.

Logo a recente situação deficitária das instituições de ensino públicas, frente à sua própria capacidade e qualidade de ensinar criou um espaço de oportunidades que gradativamente foram sendo ocupadas pelas Escolas de Ensino Privado com a busca em investimentos de ferramentas e recursos pedagógicos para a oferta de um nível de ensino cada vez mais qualificado, fruto da própria exigência de seu público que vê acirrar e se tornarem cada vez mais competitivas as vagas ou oportunidades necessárias para que seus filhos alcancem suas metas de carreira profissional.

Se as escolas particulares perceberam essa oportunidade de ganho e crescimento, as startups e as *Edtech's*[21] perceberam isso com muito mais facilidade e escalabilidade.

Todavia a grande preocupação dessas empresas de tecnologia é a entrega da escala, do resultado de análises a partir de quaisquer combinações de dados (especialmente pessoais) que com elas tenham sido compartilhados, a pretexto de dar atendimento ao processo de escolarização.

Para além disso, a preocupação regulatória, sob o aspecto a LGPD é definir as posições de agentes de tratamento, e a responsabilidades pelos ônus do contrato, sem que haja, na sua grande maioria, desde a idealização, concepção e desenvolvimento da solução proposta, a preocupação com proteção da privacidade do usuário (o aluno), negligenciando questões básicas como as de *privacy by design* porque, inevitavelmente, a sua utilização envolverá o tratamento de dados pessoais, a geração de novos dados e informações que resultarão na entrega de um perfil de aluno, a partir dos resultados que ele apresentar em razão do uso dessas tecnologias, ainda mais quando eles forem crianças e adolescen-

tes, que têm proteção especial dada pelo Estatuto da Criança e do Adolescente e pela Lei Geral de Proteção de Dados, que exigem o cumprimento de requisitos específicos e impõem certos limites à forma como aquela solução deve ser a eles apresentada.

A cada dia, a tecnologia está mais presente no ambiente escolar. A pandemia impulsionou isso, com a necessidade do ensino remoto e a adoção de plataformas para a realização das atividades escolares como, por exemplo, o *Google Classroom* e *Microsoft Teams*.

Aulas foram transmitidas on-line, em salas de aula virtuais, onde os estudantes "postavam" suas atividades escolares, armazenadas não só pela própria Escola, mas também por terceiros, fornecedores de serviços de cloud (armazenamento em nuvem).

Empresas e Startups investiram nesse mercado, desenvolvendo ou aperfeiçoando soluções voltadas para o setor de Educação (*Edtech's*), propondo-se a analisar o contexto de aprendizagem e construção de conhecimento, para maximizar o entendimento de cada professor a respeito do desenvolvimento de seus alunos, de forma individualizada.

Algumas editoras de livros didáticos acompanharam esse movimento e transformaram seus livros físicos em plataformas digitais de aprendizagem, com algoritmos capazes de analisar, profundamente, a interação dos alunos em cada atividade realizada nesse novo ambiente virtual, p. ex., com as redações, registros do seu próprio aprendizado e até mesmo a realização de testes.

O crescimento e êxito do setor das *Edtech's* relaciona-se diretamente com a sua capacidade de entrega de resultados a partir da análise de dados e informações dos alunos em todo o seu contexto escolar, não apenas com métricas gerais, mas com um perfilamento (ou personificação) do corpo discente em todos os níveis de ensino, permitindo maior assertividade das Instituições de Ensino na melhoria da sua qualidade e capacidade de ensinar.

Não há nada de errado no uso de tecnologias, dados pessoais e informações que elas necessitam, desde que sejam atendidas finalidades e propósitos legítimos, alinhados à Lei de Proteção de Dados Pessoais. Mas a questão é que nem sempre as Instituições de Ensino sabem quais os dados e informações de seus estudantes e professores realmente são coletados por essas *Edtech's* e se a sua utilização está de fato limitada à contratação daquele serviço.

Não raro, nem as próprias *Edtech's* têm a noção clara dos tratamentos de dados pessoais ou daqueles que acabam gerando, quando constroem o perfil dos Estudantes e por isso deixam de empregar as camadas de segurança necessá-

rias à sua proteção. E, quando têm a real noção, não trazem isso à tona de forma clara e transparente, porque todas essas informações, principalmente as que formam o perfil comportamental de estudantes e professores, servem, p. ex., para o aperfeiçoamento dos seus algoritmos e para novos produtos e serviços, direcionados diretamente aos Estudantes e suas Famílias.

E as inovações não se limitaram aos recursos pedagógicos, foram além. Com a retomada das aulas presenciais, por exemplo, diversas escolas implementaram nos seus acessos a coleta biométrica, com a leitura de impressão digital ou facial, para controlar o fluxo de entrada e saída da comunidade escolar, realizar a marcação de presença de estudantes. "Avanços" justificados para dar maior segurança, inclusive frente aos recentes ataques às Escolas no dia 20.04.2023, celeridade e dinamismo ao dia a dia Escolar.

Mas até que ponto as Instituições de Ensino têm conhecimento de que essa operação envolve dado pessoal e qual o volume de dados pessoais sensíveis envolvidos e que, portanto, exige o atendimento de requisitos específicos e diferenciados? Será que essa era a única alternativa e a menos intrusiva? Será que todos os recursos de segurança, e até mesmo de ensino e aprendizagem são necessários e proporcionais à natureza do dado pessoal e do tipo de titular (criança e adolescente) envolvidos?

Provavelmente não e, mesmo que tais aspectos tenham sido observados, ainda assim, o uso de dados pessoais sensíveis, nesse contexto de tratamento será considerado indevido. É o que o exemplo de uma Escola na Suécia trouxe, quando foi multada em cerca de € 20.000,00, por utilizar tecnologia de reconhecimento facial para monitorizar a frequência de um pequeno grupo de estudantes na escola, sendo que o controle de presença poderia ser feito de outras maneiras que violassem menos a privacidade.

De forma geral, o uso (ou tratamento) de dados pessoais pelas Instituições de Ensino, principalmente quando envolver o seu compartilhamento com terceiros, precisa estar perfeitamente alinhado com a sua proposta pedagógica e para o cumprimento das suas obrigações assumidas para a prestação do serviço, devendo ocorrer da forma menos intrusiva à privacidade do Titular.

O mapeamento amplo e claro de todas as operações de tratamento de dados pessoais realizadas é essencial para que se dê, não só a proteção necessária, mas principalmente a devida transparência aos titulares.

A adequação dos processos, principalmente aqueles decorrentes do projeto e atividades pedagógicas, alinhada a contratos claros com definição de obrigações e responsabilidades entre Instituições de ensino e fornecedores de recur-

sos pedagógicos, sejam ou não *Edtech's*, através de termos de tratamentos de dados pessoais é indispensável.

A eficiência do processo de escolarização é essencial à sobrevivência das instituições de ensino, no caso, as particulares. Estas, em razão da alta competitividade, precisam manter os melhores índices de aprovação, de ingresso em universidades no Brasil e exterior, garantindo assim o crescimento de novas matrículas.

2.3 **diferenciações: educação particular X educação pública**

Em se tratando de escolas públicas, por disposição constitucional, o tratamento de dados de crianças e adolescentes, para o fim essencial que é a escolarização, ocorrerá em razão da hipótese legal da execução de políticas públicas que fica previsto no artigo 7º, inciso II e III, para os dados pessoais comuns e no artigo 11, inciso II, letra b para os dados pessoais sensíveis, ambos os artigos da LGPD.

Já no âmbito das escolas particulares, o cardápio de hipóteses de tratamento. Tanto dos dados pessoais de crianças e adolescentes quanto de professores, empregados e demais membros da comunidade escolar dependerão diretamente da finalidade para a qual forem coletados.

Assim, dos dados necessários para realização ou Formalização da matrícula poderá se encontrar permissão legal tanto à luz da hipótese do cumprimento de obrigação legal ou regulatória, quanto na hipótese de execução de contrato, prevista no artigo 7º, inciso V, da LGPD.

O que se quer destacar neste momento é que a LGPD não incide de uma mesma forma sobre as hipóteses de tratamento de dados ocorrentes em escolas públicas e particulares.

Em estando as escolas públicas, sob o guarda-chuva da administração pública, as hipóteses legais que mais se aproximam, sem que se exclua a possibilidade da incidência de outras são aquelas previstas no art. 7º, II e III e art. 11, II, letra b, ambos da LGPD.

Por sua vez, as escolas privadas ou particulares, para além das hipóteses legais acima, poderá ocorrer a incidência de outras hipóteses legais a autorizarem os tratamentos de dados pessoais, observado o caso em concreto, como recentemente foi esclarecido. Pela ANPD, através do seu Enunciado n.º 01/2023, em que ela afirma que o tratamento de dados pessoais de crianças e adoles-

centes poderá ser realizado com base nas hipóteses legais previstas, tanto no artigo sétimo quanto no artigo 11 da Lei Geral de Proteção de Dados, desde que observado e prevalecente o melhor interesse da criança e do adolescente a ser avaliado no caso concreto, nos termos do artigo 14 da mesma lei.

3 **considerações finais**

Antes de se pensar num projeto e adequação para uma instituição de ensino é necessário conhecer o seu ambiente regulatório cercado de Leis, resoluções e pareceres dos respectivos sistemas de ensino, outras normas que lhe são transversais, mas principalmente, sua realidade operacional, possível através de um mapeamento amplo e claro de todas as operações de tratamento de dados pessoais realizadas para que se dê, não só a proteção necessária àquele estudante ao longo da caminhada escolar, mas principalmente ao longo de toda a sua vida, garantindo que tais informações não venham a ser utilizadas em um futuro próximo.

O uso de dados pessoais para além da finalidade informada e sem base legal que a justifique é indevido e pode gerar responsabilidades financeiras às Instituições de Ensino e dado à sua imagem reputacional.

A adequação dos processos, principalmente aqueles decorrentes do projeto e atividades pedagógicas, alinhada a contratos claros com definição de obrigações e responsabilidades entre Instituições de Ensino e Fornecedores de Produtos e Serviços é condição essencial para a complementação de um ambiente Educacional seguro e de conformidade com a LGPD, para a garantia da privacidade de toda a comunidade escolar, principalmente dos estudantes (crianças e adolescentes) que têm proteção especial assegurada por essa Lei.

Para além disso, é preciso pensar na proteção desses mesmos dados pessoais para após o fim da formação escolar do aluno, a conclusão do ensino médio porque, como visto na obra de Cathy O'Neil dados pessoais dessa natureza são utilizados para alimentar algoritmos voltados para ranquear os melhores estudantes universitários, contudo sempre mantendo a opacidade na tomada daquela decisão automatizada.

referências bibliográficas

Instituto Alana. Disponível em: alana.org.br. Acesso em: 17 nov. 2023.

Presidência da República. Lei Federal n. 13709, de 13 de agosto de 2018. **Diário Oficial da União**.

Presidência da República. Lei Federal n. 8069, de 12 de julho de 1990. **Diário Oficial da União**.

Presidência da República. Lei Federal n. 9394, de 19 de dezembro de 1996. **Diário Oficial da União**.

Presidência da República. Lei Federall n. 14533, de 10 de janeiro de 2023. **Diário Oficial da União**.

Secretaria Nacional dos Direitos da Criança e do Adolescente. Brasil. Disponível em: https://www.gov.br/participamaisbrasil/mmfdh-secretaria-nacional-dos-direitos-da-crianca-e-do-adolescente. Acesso em: 17 nov. 2023.

BRASIL. **Constituição**. República Federativa do Brasil de 1988. Brasília, DF. Senado Federal, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/ConstituicaoCompilado.htm. Acesso em: 21 dez. 2023.

BROCHADO TEIXEIRA, Ana Carolina (Coord.); FALEIROS JÚNIOR, José Luiz De Moura (Coord.); DENSA, Roberta (Coord.). **Infância Adolescência e Tecnologia**: O ECA na Sociedade da Informação. Indaiatuba/SP: FOCO, 2022.

DE MELO SILVEIRA, Ana Cristina. **A proteção da criança e do adolescente no mundo digital**: O compliance como medida preventiva ao cyberbullying. Belo Horizonte: D'Plácido, 2023.

EPISÓDIO 115: **O Futuro dos Dados de Crianças no Brasil**. [Locução de]: Dadocracia. [S.l.], 4 nov. 2022 *Podcast*. Disponível em: spotify.com. Acesso em: 21 dez. 2023.

EPISÓDIO 122: **Impacto das Bigtech's na Educação Básica e Superior**. [Locução de]: Dadocracia. [S.l.], 3 mar. 2023 *Podcast*. Disponível em: spotify.com. Acesso em: 15 nov. 2023.

EPISÓDIO 126: **Violência nas escolas e regulamentação de plataformas**. [Locução de]: Dadocracia. [S.l.], 25 abr. 2023 *Podcast*. Disponível em: spotify.com.

Acesso em: 15 nov. 2023.

EPISÓDIO 138: **Apostando a infância: jogo ou bet?** [S.l.], 12 out. 2023 *Podcast*. Disponível em: spotify.com. Acesso em: 15 nov. 2023.

EPISÓDIO 139: **Tecnologia e educação**. [S.l.] *Podcast*. Disponível em: spotify.com. Acesso em: 15 nov. 2023.

EPISÓDIO 153: **As consequências da educação plataformizada**. [Locução de]: Dadocracia. [S.l.], 31 ago. 2023 *Podcast*. Disponível em: spotify.com. Acesso em: 15 nov. 2023.

FERREIRA, Dâmares. **LGPD aplicada à educação**. 2021.

HENRIQUES, Isabella. **Direitos Fundamentais da criança no ambiente digital: O dever de garantia da absoluta prioridade**: o dever de garantia da absoluta prioridade. São Paulo/SP: Revista dos Tribunais, 2023.

MARIA, Isabela Cynthia Picolo; PICOLO. **26) AUTODETERMINAÇÃO INFORMATIVA: COMO ESSE DIREITO SURGIU E COMO ELE ME AFETA?** . Lapin. São Paulo/SP. Disponível em: https://lapin.org.br/2021/04/27/autodeterminacao-informativa-como-esse-direito-surgiu-e-como-ele-me-afeta/. Acesso em: 17 nov. 2023.

MEKE, Fabiano. **As origens alemãs e o significado da autodeterminação informativa**. Migalhas. Porto Alegre/RS, 2020. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/335735/as-origens-alemas-e-o-significado-da-autodeterminacao-informativa. Acesso em: 17 nov. 2023.

ON'NEIL, Cathy. **Algoritmos de destruição em massa**: como o big data aumenta a desigualdade e ameaça a democracia. Tradução Rafael Abraham. Santo André, SP, 2020. Tradução de: Weapons of math destriction: how big data increases inequality and treathents democracy.

TEFFÉ, Chiara Spadaccini de. **Dados Pessoais Sensíveis**: Qualificação, Tratamento e Boas Práticas. Editora Foco, f. 201, 2022. 402 p.

notas de rodapé

1 Inicialmente, gostaria de expressar meus sinceros agradecimentos ao amabilíssimo Gedeão França, pesquisador da Data Privacy Brasil (DPB), pelo gentil convite de compartilhar este capítulo, resultado da minha palestra no 4º Data Talk, evento online que reuniu diversos profissionais e pesquisadores com atuação na área de proteção de dados pessoais no 2º semestre de 2023.

2 A autodeterminação informativa está presente como um dos fundamentos da LGPD, prevista no art. 2º, sem que, contudo, a lei tenha trazido o que ela de fato signifique. Ela tem origem a partir do julgamento do caso do Censo de 1983, pela Corte Constitucional da Alemanha, em que se reconheceu, ao final que "A autodeterminação informativa pretende conceder ao indivíduo o poder, de ele próprio decidir acerca da divulgação e utilização de seus dados pessoais". Trecho do texto do Prof. Fabiano Menke, disponível em https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/335735/as-origens-alemas-e-o-significado-da-autodeterminacao-informativa. Acessado em 17.11.2023.

3 A Educação Básica, segundo a Lei de Diretrizes e Bases da Educação Nacional (LDB), Lei n.º 9.394/96, em seu artigo 4º, é obrigatória a partir dos 04 e até os 17 anos, dividindo-se nas seguintes etapas: (a) Pré-escola (de 04 até 05 anos), (b) Ensino Fundamental (Anos Iniciais, 1ª série até 5ª série e Anos Finais, 6ª séria até 9ª séria) e (c) Ensino Médio (1ª séria até 3ª série).

4 ON'NEIL, Cathy. Algoritmos de destruição em massa: como o big data aumenta a desigualdade e ameaça a democracia. Tradução Rafael Abraham. Santo André, SP, 2020. Tradução de: *Weapons of math destriction: how big data increases inequality and treathents democracy*.

5 Art. 205. A educação, direito de todos e dever do Estado e da família, será promovida e incentivada com a colaboração da sociedade, visando ao pleno desenvolvimento da pessoa, seu preparo para o exercício da cidadania e sua qualificação para o trabalho.

6 Art. 227. É dever da família, da sociedade e do Estado assegurar à criança, ao adolescente e ao jovem, com absoluta prioridade, o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária, além de colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão.

7 Art. 53. A criança e o adolescente têm direito à educação, visando ao pleno desenvolvimento de sua pessoa, preparo para o exercício da cidadania e qualificação para o trabalho, assegurando-se-lhes: I - igualdade de condições para o acesso e permanência na escola; II - direito de ser respeitado por seus educadores; III - direito de contestar critérios avaliativos, podendo recorrer às instâncias escolares superiores; IV - direito de organização e participação em entidades estudantis; V - acesso à escola pública e gratuita, próxima de sua residência, garantindo-se vagas no mesmo estabelecimento a irmãos que frequentem a mesma etapa ou ciclo de ensino da educação básica.

8 Art. 54. É dever do Estado assegurar à criança e ao adolescente: I - ensino fundamental, obrigatório e gratuito, inclusive para os que a ele não tiveram acesso na

idade própria; II - progressiva extensão da obrigatoriedade e gratuidade ao ensino médio; III - atendimento educacional especializado aos portadores de deficiência, preferencialmente na rede regular de ensino;

9 BNCC – Base Nacional Comum Curricular. A Base Nacional Comum Curricular é um documento normativo que define o conjunto de aprendizagens essenciais que todos os alunos devem desenvolver ao longo das etapas e modalidades da Educação Básica. Seu principal objetivo é ser a balizadora da qualidade da educação no País por meio do estabelecimento de um patamar de aprendizagem e desenvolvimento a que todos os alunos têm direito! Texto extraído do site http://basenacionalcomum.mec.gov.br/a-base. Acessado em 17.11.2023

10 Lei Federal n.º 14.533 de 11 de janeiro de 2023. Disponível em https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Lei/L14533.htm. Acessado em 17.11.2023

11 Art. 4º (...)XII - educação digital, com a garantia de conectividade de todas as instituições públicas de educação básica e superior à internet em alta velocidade, adequada para o uso pedagógico, com o desenvolvimento de competências voltadas ao letramento digital de jovens e adultos, criação de conteúdos digitais, comunicação e colaboração, segurança e resolução de problemas.

12 ico.org.uk

13 Os recursos são gratuitos para download e uso e estão disponíveis em https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/school-resources/

14 cnil.fr

15 https://www.cnil.fr/fr/enfants-et-ados/scolarite-et-activites-extrascolaires

16 aepd.es

17 https://www.boe.es/boe/dias/2022/07/12/pdfs/BOE-A-2022-11574.pdf. Acessado em 17.11.2023

18 dataprotection.ie

19 https://www.dataprotection.ie/sites/default/files/uploads/2022-05/DPC_MyDataProtectRights_APR22.pdf. Acessado em 17.11.2023

20 https://www.dataprotection.ie/sites/default/files/uploads/2023-03/DPC%20AR%20English_web.pdf. Acessado em 17.11.2023

21 De forma geral, *EdTech's* é o termo usado para nomear as Startups que criam soluções de hardware ou software para o Mercado de Educação, com a finalidade de auxiliar no processo de ensino e aprendizagem tanto para a Educação Básica, quanto para a de Nível Superior. É a combinação das palavras *education* e *technology* (educação e tecnologia).

A Lei Geral de Proteção de Dados - Lei Nº 13.709/2018 –, e a importância da inserção do princípio da não discriminação como contribuição para uma sociedade mais justa

Vanessa Santos

1 introdução

Técnicas de *big datas, machine learning* e inteligência artificial estão sendo cada vez mais utilizadas por governos e órgãos públicos. E assim, se torna cada vez mais comum a coleta de vários tipos de dados, inclusive biométricos, entre eles DNA, tipo de sangue, impressões digitais, gravações de voz e imagem.

E buscando estimular e facilitar o compartilhamento de dados na Administração Pública foi sancionado o Decreto Lei 10.046, em 9 de outubro de 2019, que dispõe sobre a governança no compartilhamento de dados no âmbito da Administração Pública Federal e institui o Comitê Central de Governança de Dados e o Cadastro Base do Cidadão.

E, a Lei Geral de Proteção de Dados (LGPD), Lei nº 13709, que é considerada uma política pública regulatória e que foi elaborada em 2018, mas que teve a sua total vigência iniciada recentemente, em 18 de setembro de 2020, também estabelece que:

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

> (...)
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

Também, a Constituição Federal em seu artigo 5º, garante respeito à intimidade, à vida privada, à honra e à imagem das pessoas. Tal garantia é, também, observada em diferentes marcos legislatórios como o próprio Marco Civil da Internet (Lei 12.965/2014) e a Lei de Acesso à Informação (Lei 12.527/2011), entre outros.

Porém, a forma com que os dados são tratados e colhidos pela Administração Pública na execução de políticas públicas realmente obedece ao princípio da não discriminação? Os objetivos que fizeram com que este princípio fosse incluído na LGPD estão sendo realmente alcançados?

Antes de nos direcionarmos ao princípio da não discriminação é preciso revisitarmos conceitos pensados por grandes juristas brasileiros. Sendo assim, começamos com Miguel Reale, que nos diz que:

> Princípios são, pois verdades ou juízos fundamentais, que servem de alicerce ou de garantia de certeza a um conjunto de juízos, ordenados em um sistema de conceitos relativos à dada porção da realidade. Às vezes também se denominam princípios certas proposições, que apesar de não serem evidentes ou resultantes de evidências, são assumidas como fundantes da validez de um sistema particular de conhecimentos, como seus pressupostos necessários. (REALE, Miguel. Filosofia do Direito. 11. ed. São Paulo: Saraiva, 1986. p 60).

Para Luis Roberto Barroso:

> São o conjunto de normas que espelham a ideologia da Constituição, seus postulados básicos e seus fins. Dito de forma sumária, os princípios constitucionais são as normas eleitas pelo constituinte como fundamentos ou

> qualificações essenciais da ordem jurídica que institui. (BARROSO, Luís Roberto. Interpretação e aplicação da Constituição: fundamentos de uma dogmática constitucional transformadora. São Paulo, Saraiva, 1999, pág. 147).

Por fim, Celso Antônio Bandeira de Mello, sobre os efeitos de sua inobservância:

> Princípio - já averbamos alhures - é, por definição, mandamento nuclear de um sistema, verdadeiro alicerce dele, disposição fundamental que se irradia sobre diferentes normas compondo-lhes o espírito e servindo de critério para sua exata compreensão e inteligência, exatamente por definir a lógica e a racionalização do sistema normativo, no que lhe confere a tônica e lhe dá sentido harmônico. É o conhecimento dos princípios que preside a intelecção das diferentes partes componentes do todo unitário que há por nome sistema jurídico positivo [...]. Violar um princípio é muito mais grave que transgredir uma norma qualquer. A desatenção ao princípio implica ofensa não apenas a um específico mandamento obrigatório, mas a todo o sistema de comandos. É a mais grave forma de ilegalidade ou de inconstitucionalidade, conforme o escalão do princípio atingido, porque representa insurgência contra todo o sistema, subversão de seus valores fundamentais, contumélia irremissível a seu arcabouço lógico e corrosão de sua estrutura mestra. Isto porque, com ofendê-lo, abatem-se as vigas que os sustêm e alui-se toda a estrutura nelas esforçada. (MELLO, Celso Antônio Bandeira de, Curso de Direito Administrativo. 12ª ed. – São Paulo: Malheiros, 2000, p. 747/748.)

Estes conceitos nos dizem que os princípios carregam consigo alto grau de imperatividade, o que denota o seu caráter normativo, cogente, impositivo de observância obrigatória. E o não atendimento a eles pode acarretar a ilegalidade e a inconstitucionalidade do ato do poder público, trazendo consequências desastrosas para a sociedade como um todo.

Contudo, e ao direcionarmos o nosso olhar para o princípio da não discriminação que está inserido na LGPD e que garante o tratamento adequado e igualitário dos dados pessoais, devemos nos atentar e verificar se a Autoridade Nacional de Proteção de Dados (ANPD) está criando meios adequados e diretrizes para que de fato este seja atendido pelo poder público e também privado, e tanto nos ambientes físicos como também nos virtuais.

Nos ambientes virtuais, o uso cada vez mais frequente de inteligência artificial não impede que discriminações continuem a serem reproduzidas. Pelo fato de sistemas de inteligência artificial aprenderem com dados, e por serem gerenciados por pessoas, que refletem a sociedade que vivem, isto não garante que seus resultados sejam livres de preconceito ou discriminação. Os dados usados para treinar e testar tais sistemas, e também a maneira como são projetados e usados, são todos fatores que podem levar as pessoas a serem tratadas de forma menos favorável, ou colocadas em situações de desvantagem.

Como exemplo, podemos acrescentar aqui também o uso de algoritmos para coleta e armazenamento de dados. Mas o que são algoritmos?

Segundo o artigo "Controvérsias sobre Danos Algorítmicos: discursos corporativos sobre discriminação codificada", publicado na Revista Observatório:

> Algoritmos nunca agem isoladamente (SEAVER, 2019; SILVEIRA, 2019). Definidos, em geral, como um conjunto de instruções ou regras para solucionar um problema ou para realizar uma tarefa, precisam estar em contato com uma estrutura de dados para agirem. Algoritmos integram uma rede de actantes (LATOUR, 2005). Suas conexões com dados de entrada, com o feedback, com os efeitos de suas próprias decisões e com os demais componentes dos sistemas que os implementam precisam ser considerados.
>
> (...) Esses sistemas podem ser confeccionados para seguirem regras de como executar suas ações a partir das informações que recebem. Podem ser criados para aprenderem com os dados que recebem em função dos objetivos prescritos. Também podem ter como finalidade encontrar correlações fortes nos dados que recebem. Enfim, podem criar suas operações com base nos dados e não em regras fixadas. (SILVA; SILVEIRA, 2020, p. 1/2)

Ou então, segundo a matemática e ativista Cathy O' Neil, que afirma que os algoritmos são "opiniões fechadas em matemática" (O'NEIL, 2020). Dependendo de quem construa esses modelos, quais variáveis levam em conta, e com que dados os alimente, o resultado será um ou outro. "Geralmente achamos que os algoritmos são neutros, mas não é assim. Os vieses são estruturais e sistêmicos, têm pouco a ver com uma decisão individual", explica Virginia Eubanks, professora de Ciências Políticas da Universidade de Albany (Nova York) e autora de Automating Inequality ("Automatizando a desigualdade"), um livro que investiga os vieses socioeconômicos dos algoritmos com um subtítulo significativo: *How High-Tech Tools Profile, Police, and Punish the Poor* ("como as ferramentas tecnológicas perfilam, controlam e punem os pobres").

Cathy O'Neil, em entrevista ao Portal do El País, também assevera que já é tarde para se preocupar pelo fato de que nossos dados estejam disponíveis, que agora é preciso perguntar às empresas e gigantes tecnológicos o que estão fazendo com eles. O usuário de internet não se dá conta de quando é analisado na maioria das vezes (O'NEIL, 2018). O'Neil completa o raciocínio: Quando somos conscientes de que recebemos uma pontuação de acordo com nossos dados, a primeira coisa que precisamos fazer é pedir explicações, que nos mostrem o processo pelo qual fomos qualificados, se é algo importante como uma hipoteca e um trabalho, até mesmo utilizando mecanismos legais. Às vezes em que não percebemos, são os Governos europeus e o dos Estados Unidos que precisam estabelecer normas que indiquem que a cada vez que recebemos essa pontuação precisamos saber (O'NEIL, 2018).

Dessa forma, quando para o tratamento de dados for utilizada a leitura por algoritmo, possivelmente este se baseará em um padrão, que poderá ser discriminatório, se não observada igualdade de oportunidades em razão de raça, sexo e outros dados passíveis de discriminação, que a LGPD nomeia como sensíveis.

Entre os vários exemplos práticos de casos públicos relacionados ao não atendimento ao princípio da não discriminação temos o caso da *Amazon*, que com base no histórico de contratações levou à discriminação de mulheres na seleção pela ferramenta utilizada:

> (...) a Amazon foi acusada de ter criado um algoritmo de recrutamento de novos empregados que "aprendeu" que candidatos homens eram preferíveis em detrimento das mulheres. Sobre isso, a gigante norte-americana preferiu não responder às acusações. No mesmo sentido, um estu-

> do publicado na revista Science em 2017 revela que sistemas baseados em machine learning replicam os mesmos estereótipos de gênero e raça que os humanos lutam para controlar. De onde estes estereótipos vem?
> No caso do algoritmo da Amazon, o problema se materializou porque o sistema foi treinado com currículos submetidos à análise da empresa durante os dez anos anteriores, e a maioria deles veio de homens. Ou seja, o algoritmo em si não era enviesado, mas a base de dados que foi utilizada, sim. (SARAIVA, 2019)

Ou então, podemos também utilizar outro exemplo que ocorreu no ano de 2019, onde:

> Em julho daquele mesmo ano, foi a hora da polícia do Rio iniciar seu projeto de reconhecimento facial. Escolheu-se o bairro de Copacabana como área de testes, e diversos postes foram instalados em pontos espalhados pelo bairro, devidamente equipados com câmeras nas suas extremidades. No segundo dia de testes, uma mulher foi reconhecida como sendo Maria Lêda Félix da Silva, condenada por homicídio e procurada pela polícia. Imediatamente os policiais conduziram a mulher que dizia não ser a procurada, mas estava sem documentação, até a delegacia. O erro foi resolvido quando familiares da mulher conseguiram encontrá-la na delegacia e, de posse dos seus documentos, conseguiram provar que ela não era a mulher procurada. O caso é mais um de uma série de erros que essas tecnologias cometem, mas tem um agravante: Maria Lêda, a "procurada", já estava cumprindo pena em presídio havia quatro anos. Não só os algoritmos erraram, mas também a polícia que utilizou um banco de dados desatualizado.
> Os projetos foram avançando por estados e municípios sem encontrar muita resistência. No final de 2019 eu já tinha coletado mais de 150 prisões com o uso de reconhecimento facial, e nos casos onde havia informações, mais

> de 90% das pessoas eram negras, a maioria presas por crimes sem violência. As poucas vozes que se colocaram de maneira crítica à adoção desses algoritmos pelas polícias brasileiras não foram suficientes para que um debate nacional fosse pautado. Mas quais são os problemas?
> Algoritmos são como receitas de bolo, instruções a serem seguidas para atingir o resultado final. O que acontece é que muitos desses códigos são criados com base em grandes bancos de dados por meio do aprendizado de máquina. No caso do reconhecimento facial, um grande banco de imagens de rostos é usado para ensinar o algoritmo a identificar o que é um rosto. (NUNES, 2021)

Como consequência de uma sociedade que ainda discrimina gêneros, sexualidade e raça, é mais que urgente que seja verificado se as novas ferramentas tecnológicas ou analógicas realmente contribuem para a diminuição desta realidade discriminatória. E a LGPD, poderá contribuir muito para o decréscimo dos altos índices que colocam o Brasil entre os países que mais discriminam.

Em nosso ordenamento jurídico brasileiro há diversos dispositivos que defendem a não discriminação, além daquele previsto pela LGPD, como o princípio da não discriminação (art. 3º, inciso IV, da Constituição Federal), o princípio da igualdade formal (art. 5º da Carta Magna), a Convenção sobre os Direitos das Pessoas com Deficiência (art. 2º e art. 5º), a Lei Brasileira de Inclusão (art. 4º), a Lei Geral de Proteção de Dados (art. 6º, IX), dentre outros.

Mesmo com todas estas legislações que coíbem a discriminação "pode ser extremamente difícil descobrir se os seres humanos cometeram atos discriminatórios ou não. Isso porque as pessoas podem dissimular-se ou até, em muitos casos, nem saberem que cometeram ou sofreram um ato discriminatório" (BABO, 2020).

Porém, quando direcionamos o nosso olhar para a sistematização das leis que nos protegem das discriminações negativas, ou seja, daquelas ilícitas e abusivas, fica mais fácil frearmos a manutenção de uma sociedade que há tempos possui arraigada em sua base a institucionalização e naturalização de suas desigualdades. Nesse caso, parece mais fácil lidarmos com sistemas do que com pessoas. No entanto, enquanto não contribuirmos para uma sociedade mais diversa, igualitária e equânime, os sistemas continuarão a refletir as diferenças, já que quem os criam e gerenciam são pessoas.

Deste modo, e para que haja de fato uma contribuição significativa desta lei, se torna urgente acompanharmos se o princípio da não discriminação está sendo de fato atendido. O referido princípio, está previsto no artigo 6º da LGPD que nos diz:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> (...)
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

E não só no Brasil como em um número significativo de países, governos ao redor do globo perceberam a necessidade de regulamentação, controle e fiscalização das práticas e políticas antidiscriminatórias relacionadas aos dados pessoais.

> A Comissão da União Europeia foi a primeira a perceber a necessidade crescente de proteger seus cidadãos e garantir a eles seus direitos referentes à proteção de dados pessoais. O fez por meio do Regulamento Geral sobre a Proteção de Dados (GDPR, sigla em inglês) (COSTA, 2019, p. 2)

Importante dizer que a LGPD é fruto do Regulamento Geral sobre a Proteção de Dados (sigla em inglês GDPR 2016/679), que é um regulamento do direito europeu sobre privacidade e proteção de dados pessoais, aplicável a todos os indivíduos na União Europeia e que é também fonte de inspiração direta da referida lei brasileira de proteção de dados. E o princípio da discriminação foi incluído no regulamento europeu devido a vários fatores, mas o mais famoso deles se refere à utilização incorreta de dados em um Hospital acusado de usar critérios misóginos e xenófobos na admissão de seus funcionários. Pois:

> Nas décadas de 1970 e 1980, o St. George's Hospital Medical School, no Reino Unido, utilizou um programa desenvolvido para realizar uma triagem inicial dos solicitantes. O programa, que imitava as escolhas que a equipe havia feito no passado, negou entrevistas a 60 candidatos, porque eram mulheres ou porque tinham nomes que não

> eram de origem europeia. (VIDOR, 2019)

Se em 1970 na Europa, estudos comprovaram a utilização de dados pessoais para discriminar, a consequência disso no Brasil tem efeito devastador até os dias atuais. Pois a discriminação ainda está presente nas oportunidades de emprego, em questões de moradia, segurança, saúde, crédito e consumo.

Após a publicação do regulamento europeu, foi a vez do Estado Norte-Americano da Califórnia (STATE OF CALIFORNIA, 2018) e do Brasil, de redigirem suas Leis Gerais de Proteção de Dados. No Brasil, o Marco Civil da Internet foi a reação primária à necessidade de regulamentação da proteção de dados pessoais. Embora fosse genérico, constituiu uma base para futuros debates e regulamentações sobre o tema.

Porém, apesar destas legislações já existirem, ainda aguardamos orientações da Autoridade Nacional de Proteção de Dados para que ocorra o adequado atendimento ao referido princípio. As orientações que serão publicadas, contribuirão na formulação e implementação de políticas públicas que estarão inseridas neste novo cenário de proteção e privacidade de dados pessoais e que certamente contribuirão para a diminuição de desigualdades de tratamento discriminatório.

E diante da importância de se proteger os dados pessoais foi aprovada no dia 31 de agosto de 2021 na Câmara dos Deputados a Proposta de Emenda à Constituição (PEC) 17/19, que foi elaborada pelo Senado Federal, o que torna a proteção de dados pessoais, inclusive nos meios digitais, um direito fundamental, ou seja, se pretende assim que seja garantido a todos o mínimo necessário para que o indivíduo exista de forma digna dentro de uma sociedade administrada pelo Poder Estatal.

Segundo José Afonso Silva,

> Direitos fundamentais do homem constitui a expressão mais adequada a este estudo, porque, além de referir-se a princípios que resumem a concepção do mundo e informam a ideologia política de cada ordenamento jurídico, é reservada para designar, no nível do direito positivo, aquelas prerrogativas e instituições que ele concretiza em garantias de uma convivência digna, livre e igual de todas as pessoas.

Desta maneira, o reconhecimento da proteção de dados pessoais como direito fundamental, legitima um dos objetivos da Lei Geral de Proteção de Dados, previsto em seu artigo 1º, que nos assegura o livre desenvolvimento da personalidade, a liberdade e a privacidade.

2 **considerações finais**

Como nos diz a filósofa Carissa Véliz em entrevista intitulada de "'Falta de privacidade mata mais que terrorismo': o surpreendente alerta de professora de Oxford", concedida no dia 16 de outubro de 2020 à BBC News Brasil:

> A privacidade é importante porque a falta dela dá aos outros imenso poder sobre nós. Quando outras pessoas sabem muito sobre nós, elas podem interferir em nossas vidas.
> A privacidade nos protege de abusos de poder. Por exemplo, ele nos protege contra a discriminação. Se seu chefe não souber a religião que você segue, ele não poderá discriminá-lo.
> A privacidade é como a venda que cobre os olhos da Justiça para que o sistema nos trate com igualdade e imparcialidade.
> Neste momento, não somos tratados como iguais: não vemos o mesmo conteúdo online, não nos são oferecidas as mesmas oportunidades, muitas vezes não pagamos o mesmo preço pelos mesmos produtos — graças a algoritmos de sites da internet que usam nossos dados para nos oferecerem informações e produtos diferentes.

Desta forma, tudo o que fazemos é controlado por vários tipos de empresas, independentemente de elas serem públicas ou privadas, e por isso devemos cobrar o cumprimento da LGPD para garantirmos a devida proteção aos dados pessoais das pessoas naturais.

Contudo, o Direito ao inserir em seu ordenamento a LGPD, ainda não provê de mecanismos suficientes para absorvê-la e assim contribuir efetivamente com o seu pleno funcionamento. Utilizando de pesquisa bibliográfica em dou-

trina correspondente e jornais que comprovam os fatos suscitados, bem como por meio de uma análise crítica à legislação já existente no país, referida lei deve influenciar o cotidiano brasileiro, bem como as medidas que devem ser adotadas pelo governo no que tange à efetivação de políticas públicas baseadas na proteção e privacidade de dados.

Assim, a LGPD traz muitos desafios aos titulares de dados, aos poderes públicos e privados, à Autoridade Nacional de Proteção de Dados (ANPD) e aos operadores do Direito. Destaca-se a Autoridade Nacional de Proteção de Dados Pessoais, criada pela Medida Provisória n. 869, de 27 de dezembro de 2018, cuja conversão em lei foi aprovada pelo Senado Federal em maio de 2019, cuja competência regulatória impõe uma série de medidas para que se proceda a normatização de técnicas e orientações para atendimento à LGPD.

A atuação da ANPD é peça chave para a efetivação e atendimento amplo da LGPD, e por isso, ao analisar os próximos passos desta autoridade, devemos verificar quais medidas serão desenvolvidas para que seja atendido o princípio da não discriminação. Somente assim conseguiremos constatar se os dados pessoais – por seu potencial de identificar um sujeito – estariam ou não sendo protegidos de forma efetiva para diminuir desigualdades decorrentes de discriminações.

Trata-se, portanto, de tema relevante e pertinente em vista da possibilidade de contribuição para o fomento e implementação de políticas públicas que atendam a essa nova realidade de segurança, proteção e privacidade de dados.

referências bibliográficas

BABO, Gustavo Schainberg S. **Discriminação Algorítmica: Origens, Conceitos e Perspectivas Regulatórias**. Disponível em: https://www.dtibr.com/post/discrimina%C3%A7%C3%A3o-algor%C3%ADtmica-origens-conceitos-e-perspectivas-regulat%C3%B3rias-parte-2. Acesso em: 05 de setembro de 2021.

BARROSO, Luís Roberto. **Interpretação e aplicação da Constituição: fundamentos de uma dogmática constitucional transformadora**. São Paulo, Saraiva, 1999.

BARROSO, Luiz Roberto. **Razoabilidade e isonomia no direito brasileiro**. *In*: Viana, Márcio Túlio; Renault, Luiz Otávio Linhares (Org.). Discriminação. São Paulo: LTr, 2000.

BRASIL. **Constituição (1988)**. Constituição da República Federativa do Brasil. Brasília, DF. Senado Federal: Centro Gráfico,1988.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, DF. Publicação em 24 abr, 2014.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados. Diário Oficial da União, Brasília, DF. Publicação em 15 ago, 2018.

COSTA, Leonardo Portugal da. **A construção da Lei Geral de Proteção de Dados e seus efeitos para o Pequeno Empresário e para o Cidadão**. Disponível em: https://app.uff.br/riuff/bitstream/1/13068/1/Leonardo%20Portugal.pdf. Acesso em: 20 nov, 2020.

EUBANKS, Virginia. **Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor**. Nova York: St. Martin's Press, 2018.

MELLO, Celso Antônio Bandeira de. **Curso de Direito Administrativo**. 12ª ed. – São Paulo: Malheiros, 2000.

NUNES, Pablo. **O Algoritmo e Racismo nosso de cada dia - Reconhecimento facial aposta no encarceramento e pune preferencialmente população negra**. Disponível em: https://piaui.folha.uol.com.br/o-algoritmo-e-racismo-nosso-de-cada-dia/ Acesso em: 18 nov, 2020.

O'NEIL, Cathy. **Assim os algoritmos perpetuam a desigualdade social**. Portal

El País– 17 abr. 2018. Entrevista concedida da Patrícia Peiró. Disponível em: https://brasil.elpais.com/brasil/2018/04/12/tecnologia/1523546166_758362.html . Acesso em: 04 set. 2021.

O'NEIL, Cathy. **Weapons of math destruction: how big data increases inequality and threatens democracy**. Nova York: Broadway Books, 2016.

REALE, Miguel. **Filosofia do Direito**. 11. ed. São Paulo: Saraiva, 1986.

SARAIVA, Raquel. **Discriminação de gênero embutida em algoritmos**. 2019. Disponível em: https://ip.rec.br/2019/03/08/discriminacao-de-genero-embutida-em-algoritmos/. Acesso em: 21 dez, 2020.

SILVA, José Afonso. **Curso de Direito Constitucional positivo**. 25. ed. São Paulo: Malheiros Editores, 2005.

SILVA, Tarcizio Roberto da; SILVEIRA, Sergio Amadeu da. **Controvérsias sobre Danos Algorítmicos: discursos corporativos sobre discriminação codificada**. *In*: Revista Observatório e-ISSN nº 2447-4266, Vol.6, n.4, Julho - Setembro. 2020.

VÉLIZ, Carissa. **'Falta de privacidade mata mais que terrorismo': o surpreendente alerta de professora de Oxford**. Disponível em: https://epocanegocios.globo.com/Mundo/noticia/2020/10/falta-de-privacidade-mata-mais-que-terrorismo-o-surpreendente-alerta-de-professora-de-oxford.html. Acesso em: 15 jul, 2021.

VIDOR, Daniel Martins. **LGPD e Big Data: discriminação e invasões de privacidade – parte 1**. Disponível em: https://www.plugar.com.br/lgpd-e-big-data-discriminacao-e-invasoes-de-privacidade-parte-1/. Acesso em: 01 nov, 2020.

SEÇÃO III

Privacidade & Proteção de Dados na Infância e Adolescência

Hipóteses legais aplicáveis ao tratamento de dados de crianças e adolescentes

Juliana Brasileiro

1 introdução

A Revolução Digital decorrente da popularização dos computadores e da internet, bem como do desenvolvimento das tecnologias da informação e comunicação impactou profundamente a vida em sociedade, gerando uma nova estrutura social dominante - a sociedade em rede (DONEDA, 2019). Nesse novo modelo, a informação transformou-se no elemento central para o desenvolvimento da economia e geração de riquezas, fazendo com que o tratamento de dados pessoais passasse a ser realizado em larga escala não só pelo Estado, mas também, e cada vez mais, pelo setor privado (BIONI, 2020).

Como não poderia ser diferente, os dados de crianças e adolescentes estão inseridos nesse cenário, tendo em vista que eles também vivenciam esse novo modelo de sociedade hiperconectada. Embora o acesso à internet e às novas tecnologias esteja atrelado a uma gama infindável de recursos e possibilidades para a promoção e o exercício de direitos por crianças e adolescentes, o ambiente digital traz riscos inerentes (DE TEFFÉ, 2022).

Assim, ao interagirem em redes sociais, realizarem compras na internet, participarem de jogos digitais ou mesmo utilizarem ferramentas de ensino à distância, crianças e adolescentes disponibilizam

seus dados pessoais na rede, os quais são processados para diversos fins, nem sempre éticos ou morais. A maior suscetibilidade de crianças e adolescentes sofrerem abusos e violações de direitos no ambiente digital trouxe à baila a necessidade de um maior controle regulatório do tratamento de dados de menores.

A partir do reconhecimento da vulnerabilidade de crianças e adolescentes, decorrente da circunstância de serem pessoas em desenvolvimento e lhes faltar o completo discernimento, a Constituição Federal e o Estatuto da Criança e Adolescentes estabeleceram os princípio da Proteção Integral e da Prioridade Absoluta, dos quais decorre o da Prevalência do Melhor Interesse do Menor.

A Lei Geral de Proteção de Dados (LGPD) não ficou alheia a essa necessidade de proteção diferenciada, dedicando uma seção específica para dispor sobre o tratamento de dados de crianças e adolescentes. A novel lei prevê que "o tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.[1]" Diante do texto normativo, discute-se quais seriam as hipóteses legais aplicáveis ao tratamento de dados de crianças e adolescentes.

2 **bases legais aplicáveis ao tratamento dos dados de crianças e adolescentes**

A LGPD disciplina o tratamento de dados de crianças e adolescentes em seu art. 14, o qual estabelece que "o tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente"[2]. Ademais, dispõe que "o tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.[3]"

A referida previsão legal suscitou dúvida, discutindo-se se o §1º do art. 14 da lei seria aplicável ou não aos adolescentes. Embora não se pretenda analisar a questão neste artigo, parece que a intenção do legislador foi reconhecer a validade do consentimento do adolescente no que concerne ao tratamento de seus dados, numa hipótese de capacidade especial (DE TEFFÉ, 2022), em que pese existir entendimento em sentido contrário (HENRIQUE, PITA e HARTUNG, 2021).

Além disso, a norma suscita também dúvida quanto à possibilidade de aplicação de outras bases legais previstas na LGPD para o tratamento de dados de menores. Numa posição bastante restritiva, há corrente, segundo a qual o tratamento de dados de crianças e adolescentes apenas poderia ocorrer mediante o

consentimento dos pais ou responsável e na situação específica prevista no §3º do art. 14.

Contudo, essa corrente estaria atrelada a uma concepção de que haveria certa prioridade ou preferência pela base legal do consentimento. Entretanto, o entendimento desta autora, o qual acompanha o posicionamento da doutrina majoritária[4], é o de que inexiste hierarquia entre as bases legais, devendo ser escolhida aquela que melhor se adeque às circunstâncias concretas do tratamento.

Nessa direção, é o Enunciado no 689 da IX Jornada de Direito Civil do Conselho da Justiça Federal: "Não há hierarquia entre as bases legais estabelecidas nos art. 7º e 11 da Lei Geral de Proteção de Dados (Lei 13.709/2018)" que representa um consenso entre operadores do direito e doutrinadores.

A avaliação da adequação da base legal do consentimento precisa ser contextualizada, a fim de verificar se no caso concreto ele representará a manifestação da escolha individual no exercício de sua autonomia privada (DONEDA, 2020). Por isso, nem sempre a coleta do consentimento dos pais ou responsável será apropriada, por não representar, em todos os casos, um instrumento de escolha real.

Basta pensarmos na situação de o tratamento de dados decorrer de uma exigência legal. Nesse sentido, entendermos que o tratamento dos dados somente poderia ocorrer mediante o consentimento parental significaria que os pais ou responsável legal poderiam escolher cumprir ou não a lei, o que obviamente não pode ser aceito. Por outro lado, se não há possibilidade de escolha, não faz sentido se falar em consentimento, de modo que, nessa situação, a base apropriada poderia ser o cumprimento de obrigação legal ou regulatória pelo controlador, prevista no inciso II do art. 7º e na alínea a do inciso II do art. 11 da LGPD.

É preciso lembrar que o escopo do consentimento é garantir a autodeterminação informativa e, no caso de tratamento de dados de crianças e adolescentes, permitir que os pais ou responsável legal exerçam o controle sobre o fluxo e o destino dos dados de seus filhos ou pupilos, de modo que, não faz sentido se falar em consentimento quando inexistir possibilidade real de escolha.

Por isso, algumas questões devem ser ponderadas, a fim de se evitar situações nas quais o consentimento seja meramente formal. Nesse sentido, a base legal do consentimento não será válida sempre que, na situação concreta, os pais ou responsável não tiver real possibilidade de escolha quanto ao tratamento de dados, ou ele não puder recusar, nem revogar o consentimento, uma vez que nessas circunstâncias a manifestação de vontade não será livre.

Deste modo, precisa ser avaliado o equilíbrio de poder entre as partes, pois muitas vezes em relações verticalizadas, os pais ou responsável não têm poder real de escolha. É o que constatamos nos tratamentos de dados pelo Poder Público, nas relações de trabalho e de consumo (TEFFÉ, 2022). O cerne do adjetivo livre é verificar o grau de assimetria de poder, que poderia minar a voluntariedade do consentimento (BIONI, 2020).

Por outro lado, o consentimento também não deve ser considerado válido, quando a execução de um contrato ou a prestação de um serviço depender da concordância dos pais ou responsável com o tratamento dos dados de seus filhos ou pupilos, pois isso poderia impedir a manifestação livre da vontade[5].

Como bem observa Chiara de Teffé, "em alguns contextos, evitar a base legal do consentimento pode gerar uma proteção mais efetiva dos dados pessoais, especialmente diante de relações assimétricas (imbalance of power) com elevado potencial de risco de abuso de poder" (2022, p. 154).

Por conseguinte, essa corrente parte da ilusória concepção de controle real e efetivo por meio do consentimento parental, o que nem sempre é possível nos ambientes virtuais. Ademais, transferiria a eles a responsabilidade exclusiva de avaliar se o tratamento atende ao melhor interesse do menor, sem que tenham, muitas vezes, na prática, reais condições de realizar esse julgamento. Diante disso, não parece aceitável que o legislador tenha condicionado, sempre e em todos os casos, o tratamento dos dados de crianças e adolescentes ao consentimento dos pais ou responsável.

Paralelamente a esse posicionamento, existe corrente que defende a utilização das outras bases legais previstas para o tratamento dos dados sensíveis, constantes no §1º do art. 11 da LGPD.

Segundo esse entendimento, haveria uma similaridade de situação no tratamento dos dados sensíveis e no de dados de crianças ou adolescentes, uma vez que, em ambos os casos, o processamento seria crítico, em razão da vulnerabilidade de seus titulares. Enquanto no primeiro caso, a vulnerabilidade decorre da qualidade dos dados, cujo tratamento tem um maior potencial de causar danos ou gerar discriminações; no segundo, a vulnerabilidade é do próprio titular, tornando-os mais sujeitos a sofrer danos e violações de direitos. Portanto, essa corrente conclui que os dados de crianças e adolescentes deveriam ser considerados dados sensíveis.

Contudo, essa corrente esbarra no próprio texto normativo. Isto porque, no inciso II do art. 5º, a LGPD elenca espécies de dados sensíveis, não incluindo os dados de crianças e adolescentes nesse rol, bem como disciplina o tratamento

de dados sensíveis e o de crianças ou adolescentes em seções diferentes, evidenciando a opção do legislador de não considerar os dados de menores como dados sensíveis. Ademais, essa interpretação da lei geraria restrições ao tratamento de dados de menores, sem a existência de expressa previsão nesse sentido.

Entende-se que a pretensão do legislador foi apenas dizer que, quando a hipótese legal para o tratamento de crianças ou adolescentes for o consentimento, este deverá ser dado por um dos pais ou pelo responsável legal. Essa disposição, entretanto, não exclui a possibilidade de aplicação das outras bases legais previstas no art. 7º ou no art. 11 da lei, quando se tratar, respectivamente, de dados pessoais ou dados sensíveis.

O que precisa ser compreendido é que a eleição da melhor base legal para o tratamento de dados de crianças e adolescentes depende de uma avaliação cuidadosa acerca de sua adequação à finalidade do tratamento e às características da situação concreta, sempre guiada pelo melhor interesse do menor, o qual deve sempre prevalecer.

Visando uniformizar a interpretação da LGPD, Autoridade Nacional de Proteção de Dados publicou o Enunciado no 1, pelo qual "O tratamento de dados pessoais de crianças e adolescentes poderá ser realizado com base nas hipóteses legais previstas no art. 7º ou no art. 11 da Lei Geral de Proteção de Dados Pessoais (LGPD), desde que observado e prevalecente o seu melhor interesse, a ser avaliado no caso concreto, nos termos do art. 14 da Lei."

3 **considerações finais**

A escolha da hipótese legal para determinada operação de tratamento de dados de crianças e adolescentes depende de uma investigação cautelosa acerca de sua adequação à finalidade do tratamento e às características da situação concreta, observando sempre o melhor interesse do menor. Este sim é o critério inegociável que pode e deve limitar a exploração dos dados de crianças e adolescentes, quando a finalidade perseguida pelo agente de tratamento colidir com o melhor interesse do menor.

Nesse sentido, é preciso sempre lembrar que a LGPD tem o escopo geral de proteger os direitos fundamentais de liberdade e de privacidade, bem como o livre desenvolvimento da personalidade da pessoa natural. Adicionalmente, no caso específico de tratamento de dados de crianças ou adolescentes, a lei deixa evidente a intenção de sempre proteger o interesse do menor, dando-lhe preva-

lência sobre qualquer outro interesse em jogo no caso concreto.

Posto isso, quando a base legal do consentimento não servir a esses propósitos, deve ser analisada a adequação das outras bases legais previstas no art. 7º ou no art. 11 da LGPD.

referências bibliográficas

BIONI, Bruno Ricardo, **Proteção de Dados Pessoais:** a função e os limites do consentimento, 2ª edição, Forense, Rio de Janeiro, 2020.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei no 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da República Federativa do Brasil, Poder Legislativo, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 12 março 2023.

CONSELHO EUROPEU. **Regulamento (UE) no 2016/679 do Parlamento Europeu e do Conselho, de 23 de abril de 2016**, relativa 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). Jornal Oficial da União Europeia, Estrasburgo, 04/05/2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 10/03/2023.

DONEDA, Danilo, **Da privacidade à proteção de dados pessoais**: fundamentos da Lei geral de proteção de dados, 2a edição, Revista dos Tribunais, São Paulo, 2019.

HENRIQUE. Isabella; PITA, Marina; HARTUNG, Pedro, **A Proteção de Dados Pessoais de Crianças e Adolescentes**, *in*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Wolfgang; RODRIGUES JR., Otávio Luiz (coord.), Tratado de Proteção de Dados Pessoais, 1ª edição, Forense, Rio de Janeiro, 2021, p. 199-224.

TEFFÉ, Chiara Spadaccini de, Dados pessoais sensíveis: qualificação, tratamento e boas práticas, 1ª edição, Foco, Indaiatuba, 2022.

notas de rodapé

1 Art. 14, §1º da Lei 13.709/2018.

2 Art. 14 da Lei 13.709/2018.

3 Art. 14, §1º da Lei 13.709/2018.

4 A exemplo de TEFFÉ, Chiara Spadaccini de; BIONI, Bruno; SCHERTEL, Laura, entre outros.

5 Guidelines 05/2020 on consent under Regulation 2016/679, p. 7. Disponível em: <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf>. Acesso em: 25 Fev. 2023..

Reconhecimento facial de crianças e adolescentes: limites e cuidados

Franklin Jeferson

Pollyana Moreira

1 introdução

A evolução tecnológica tem proporcionado avanços notáveis, principalmente com a utilização do reconhecimento facial, um sistema que se dedica à identificação e autenticação de indivíduos por meio das características únicas e distintivas de seus rostos. Apesar de sua versatilidade e relevância, essa tecnologia encontra-se no cerne de debates intensos, especialmente em um contexto em que as regulamentações das tecnologias de inteligência artificial ganham cada vez mais destaque.

No epicentro dessas controvérsias, surge uma discussão crucial que vai além do entendimento puramente técnico e penetra nas esferas éticas e legais. Em meio a esse cenário, torna-se imperativo abordar a crescente utilização do reconhecimento facial, especialmente quando aplicado no ambiente escolar, e direcionar a atenção para uma questão sensível e premente: a utilização dessa tecnologia em crianças e adolescentes.

Neste contexto, é essencial considerar não apenas os aspectos técnicos do reconhecimento facial, mas também os desafios éticos e legais inerentes ao seu emprego em ambientes educacionais. A proteção da privacidade, o desenvolvimento psicossocial dos jovens e as potenciais consequências a longo prazo demandam uma abordagem reflexiva e cuidadosa.

Diante do quadro, a investigação inicial não pre-

tende demonstrar todos os normativos criados no Brasil que tratam, de algum modo, sobre a temática, mas busca suscitar sobre os cuidados da utilização do reconhecimento facial de crianças adolescentes, de forma a contribuir para um diálogo informado e responsável acerca da adoção desta tecnologia em ambientes educacionais, ponderando sobre os possíveis impactos em relação ao desenvolvimento e à privacidade desses indivíduos.

Para tanto apresenta-se o dever de proteção e o problema contemporâneo vivenciado, seguido de uma análise bibliográfica sobre a utilização da tecnologia de reconhecimento facial no âmbito educacional e considerações finais.

2 **desenvolvimento**

2.1 **proteção de dados no brasil: um olhar sobre crianças e adolescentes**

A proteção de dados no Brasil emerge em meio a um cenário cada vez mais digitalizado, exigindo uma análise particularmente cuidadosa quando se trata de crianças e adolescentes. Com a promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD) em 2018, o Brasil deu passos significativos na definição de diretrizes para o tratamento responsável das informações pessoais dos cidadãos. Contudo, a proteção de dados, quando aplicada a crianças e adolescentes, transcende a mera conformidade legal, adentrando um terreno sensível que envolve não apenas questões jurídicas, mas também considerações éticas e sociais.

No âmbito da LGPD, um destaque crucial é o Capítulo II Seção III que aborda de forma específica o tratamento de dados pessoais de crianças e de adolescentes. Este enfoque reflete uma compreensão crescente sobre a importância de salvaguardar os direitos e a privacidade das crianças em um ambiente digital cada vez mais presente em suas vidas. Neste contexto, a Autoridade Nacional de Proteção de Dados (ANPD) desempenha um papel crucial na orientação e fiscalização das práticas de tratamento de dados, proporcionando clareza sobre as interpretações legais e buscando assegurar que o processamento de informações de crianças e adolescentes seja sempre realizado em conformidade com os princípios da LGPD e, acima de tudo, em seu melhor interesse.

Diante da considerável complexidade do tema, a Autoridade Nacional de Proteção de Dados emitiu o enunciado CD/ANPD nº1, datado de 22 de maio de 2023, o qual esclareceu que o tratamento de dados de crianças e adolescentes poderá, além do consentimento, ser realizado utilizando as hipóteses legais

previstas no art. 7º ou no art. 11 da LGPD, "desde que observado e prevalecente o seu melhor interesse, a ser avaliado no caso concreto, nos termos do art. 14 da Lei." É importante analisarmos o que se pretende dizer com a expressão "melhor interesse da criança e adolescente", nesse sentido faz se necessário utilizar a origem do seu conceito para posteriormente analisar sua aplicabilidade. Camila Colucci, 2014, explica[1]:

> "A origem do melhor interesse da criança adveio do instituto inglês *parens patriae* que tinha por objetivo a proteção de pessoas incapazes e de seus bens. Com sua divisão entre proteção dos loucos e proteção infantil, esta última evoluiu para o princípio do *best interest of child*."

Já o Estatuto da Criança e do Adolescente – ECA[2], em seu art. 3º e 4º, traz o seguinte:

> "A criança e o adolescente gozam de todos os direitos fundamentais inerentes à pessoa humana, sem prejuízo da proteção integral de que trata esta Lei, assegurando- selhes, por lei ou por outros meios, todas as oportunidades e facilidades, a fim de lhes facultar o desenvolvimento físico, mental, moral, espiritual e social, em condições de liberdade e de dignidade. Parágrafo único. Os direitos enunciados nesta Lei aplicam-se a todas as crianças e adolescentes, sem discriminação de nascimento, situação familiar, idade, sexo, raça, etnia ou cor, religião ou crença, deficiência, condição pessoal de desenvolvimento e aprendizagem, condição econômica, ambiente social, região e local de moradia ou outra condição que diferencie as pessoas, as famílias ou a comunidade em que vivem." "É dever da família, da comunidade, da sociedade em geral e do poder público assegurar, com absoluta prioridade, a efetivação dos direitos referentes à vida, à saúde, à alimentação, à educação, ao esporte, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária".

Não obstante, a Constituição Federal, aborda em seu Capítulo II, art. 15, "que a criança e o adolescente têm direito à liberdade, ao respeito e à dignidade como pessoas humanas em processo de desenvolvimento e como sujeitos de direitos civis, humanos e sociais garantidos". Tal direito constitucional, reflete na importância de proporcionar um ambiente propício ao desenvolvimento integral da criança e do adolescente, incluindo não apenas questões de liberdade e dignidade, mas também abrangendo aspectos como educação, saúde, lazer e proteção contra qualquer forma de exploração ou violência.

Sendo assim, as legislações no Brasil buscam não apenas reconhecer formalmente os direitos das crianças e adolescentes, mas também efetivar mecanismos que assegurem a implementação desses direitos na prática, contribuindo para a formação de cidadãos conscientes, saudáveis e plenamente integrados à sociedade.

2.2 **reconhecimento facial no âmbito educacional**

De acordo com os documentos legais, mencionados anteriormente, torna-se essencial zelar pelos interesses primordiais de crianças e adolescentes, ao mesmo tempo em que se busca compreender de que forma tais direitos podem ser adequadamente protegidos e respeitados no cenário digital. Diante da notável quantidade de dados pessoais tratados pelas instituições educacionais, incluindo os de crianças e adolescentes, surge a legítima preocupação sobre se tais entidades estão devidamente priorizando a adoção de cuidados apropriados durante o processo de tratamento dessas informações.

Conforme pesquisa sobre mapeamento das políticas de reconhecimento facial em escolas públicas brasileiras[3], elaborado pelo Internetlab, as finalidades elencadas pelos poderes locais para a implementação da tecnologia concentram-se, em três grupos: Otimização da gestão do ambiente escolar; Combate à evasão escolar e segurança. Ressalta-se que no estudo realizado, nenhum dos municípios listados na pesquisa citada relatou a realização de relatório de impacto à proteção de dados pessoais ou análises sobre o potencial de discriminação resultante de softwares de reconhecimento facial. Além disso, o relatório indicou limitações no uso de soluções tecnológicas para abordar problemas estruturais na educação pública brasileira, especialmente devido aos riscos associados ao emprego de tecnologias invasivas, como o reconhecimento facial.

Sobre a utilização desta tecnologia, destaca-se também o Relatório sobre Re-

conhecimento facial nas escolas públicas no Paraná, publicado em dezembro de 2023, o qual menciona sobre o pedido de informação ao Ministério dos Direitos Humanos (MDH) e os riscos da utilização desta tecnologia:

> "Isto posto, o Ministério é contrário à produção de imagens de crianças e adolescentes, dados os riscos à integridade a que as crianças ficariam expostas devido à aferição de registro de frequência por aparelhos celulares e aos marcadores de pontos de expressões faciais. (MDH, 2023 apud ISRAEL, FIRMINO, 2023, p.8)"

Ainda de acordo com o relatório produzido por ISRAEL, FIRMINO, 2023, a política de privacidade do aplicativo utilizado para o reconhecimento facial nas escolas do Paraná, trata a coleta de dados biométricos como dados pessoais, não especificando que estes são dados pessoais sensíveis. Prevê também, em sua base legal para a utilização, o atendimento aos interesses legítimos do controlador, sendo esta previsão ausente na sessão que rege o tratamento de dados sensíveis.

Os exemplos e relatórios citados acima trazem ao debate os limites e cuidados da tecnologia de reconhecimento facial no ambiente escolar. O uso de reconhecimento facial nas escolas apresenta uma série de desafios, que devem ser cuidadosamente considerados antes de sua implementação. Um dos principais desafios está na garantia da privacidade de crianças e adolescentes. O debate com a sociedade tem que ser construído para o entendimento do que é a tecnologia, os riscos que esta traz e como pode ajudar no desenvolvimento educacional. A garantia da autodeterminação informativa[4] é outro desafio que tem que ser posto em discussão. Afinal, é um propósito educacional, com finalidades específicas para tal, ou um projeto de vigilância com possibilidades de desdobramentos repressores?

Atualmente está em andamento o projeto de lei 2606/2023, proposto pelo Deputado Sargento Gonçalves (PL/RN), o qual visa implementar a identificação biométrica/facial como requisito para ingresso em escolas públicas ou privadas de educação básica. A proposta propõe também a verificação por detectores de metais e estabelece a obrigação de adquirir equipamentos correspondentes. Tais medidas nos fazem pensar: Quais seriam os limites da utilização destas tecnologias? A constante vigilância, inerente ao reconhecimento facial, pode gerar impactos psicológicos avassaladores em crianças e adolescentes, principal-

mente no que diz respeito ao compartilhamento ou uso indevido de tais dados. A sensação de monitoramento constante pode afetar a autoestima, inibindo a expressão e prejudicando o desenvolvimento emocional.

A ausência de normativos específicos sobre o uso e cuidados das tecnologias de reconhecimento facial nas escolas ou no plano nacional de educação, deixa espaço para abusos. Se faz necessário estabelecer diretrizes éticas claras, considerando sempre o bem-estar e direitos fundamentais das crianças e adolescentes. A busca por um equilíbrio entre segurança e preservação dos direitos é essencial. Por fim, a implementação ética dessa tecnologia requer a participação ativa da sociedade, legisladores e educadores, tentando garantir um ambiente escolar que promova o desenvolvimento saudável, respeitando a privacidade e autonomia das crianças e adolescentes.

3 **considerações finais**

O presente trabalho teve como objetivo questionar sobre a aplicação do reconhecimento facial em ambientes educacionais, sobretudo a utilização dos dados de crianças e adolescentes. O avanço tecnológico, em especial o reconhecimento facial, é representado por ser uma ferramenta poderosa com potenciais benefícios em termos de segurança e eficiência. No entanto, ao implementar essa tecnologia nas escolas, somos confrontados com desafios significativos relacionados à privacidade, desenvolvimento psicossocial e impactos a esses titulares que ainda estão em fase de desenvolvimento.

A Lei Geral de Proteção de Dados Pessoais, estabelece diretrizes importantes para o tratamento responsável, com especial atenção para os dados de crianças e adolescentes. A emissão do enunciado CD/ANPD nº1 pela Autoridade Nacional de Proteção de Dados, reforça a necessidade de priorizar o melhor interesse desses jovens em situações específicas.

Embora este trabalho não tenha a pretensão de explorar exaustivamente a temática, busca evidenciar a relevância de uma abordagem cautelosa diante dos cuidados associados ao uso dessa tecnologia por instituições de ensino. Além dos aspectos legais, é crucial considerar os riscos envolvidos ao submeter esses estudantes ao reconhecimento facial. A tecnologia deve ser avaliada não apenas por sua eficácia, mas também por seu impacto nas experiências educacionais e no desenvolvimento individual de cada aluno.

referências bibliográficas

BRASIL. **Constituição Federal de 1988**. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 26 novembro. 2023.

BRASIL. **Lei 13.709 de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 26 novembro. 2023.

BRASIL. **Lei 8.069, DE 13 DE JULHO DE 1990**. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 26 novembro. 2023.

BRASIL. **PL 2606/2023**. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao/?idProposicao=2362562. Acesso em: 26 novembro. 2023.

BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). **ENUNCIADO CD/ANPD Nº 1, DE 22 DE MAIO DE 2023**. Disponível em: https://www.in.gov.br/en/web/dou/-/enunciado-cd/anpd-n-1-de-22-de-maio-de-2023-485306934. Acesso em: 26 novembro. 2023.

COLUCCI, Camila. **Princípio do melhor interesse da criança: construção teórica e aplicação prática no direito brasileiro**. Disponível em: <https://www.teses.usp.br/teses/disponiveis/2/2131/tde-25022015-083746/pt-br.php>. Acesso em: 26 novembro. 2023.

INTERNETLAB. **Tecnologias de vigilância e educação: um mapeamento das políticas de reconhecimento facial em escolas públicas brasileiras**. Disponível em: <https://internetlab.org.br/wp-content/uploads/2023/06/Educacao-na-mira-PT_06.pdf>. Acesso em: 26 novembro. 2023.

ISRAEL. Carolina Batista, FIRMINO. Rodrigo. **Reconhecimento facial nas escolas públicas do Paraná**. Disponível em: <https://appsindicato.org.br/wp-content/uploads/2023/12/RF_PR_2023.pdf>. Acesso em: 26 novembro. 2023.

notas de rodapé

1 Princípio do melhor interesse da criança: como definir a guarda dos filhos?

2 Estatuto da Criança e do Adolescente - ECA

3 Tecnologias de vigilância e educação – um mapeamento das políticas de reconhecimento facial em escolas públicas brasileiras

4 https://lapin.org.br/2021/04/27/autodeterminacao-informativa-como-esse-direito-surgiu-e-como-ele-me-afeta/

SEÇÃO IV

Segurança da Informação & Proteção de Dados

Segurança de Informação: cuidados básicos

Carmen Arriagada

O Data Talks, uma iniciativa da Data Privacy Brasil, é um evento do Clube Data, um espaço para discussões, conversas e trocas mais curtas, sobre diversos assuntos relacionados à privacidade e proteção de dados. A escolha do tema para esta conversa teve como intuito conciliar um pouco da prática adquirida nas formações realizadas em cursos ministrados pela Data Privacy Brasil com alguns pontos de cuidado decorrentes da prática na atuação, onde certamente o profissional da área precisa agregar conhecimentos relacionados a outras áreas.

Segundo o que dispõe o prefácio da ABNT NBR ISO/IEC 27002:2013, a segurança é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de *software* e *hardware*.

Ainda, segundo o Glossário elaborado pelo Departamento de Segurança da Informação (DSI), do Gabinete de Segurança Institucional da Presidência da República, a segurança da informação "trata de ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações"[1]. Acrescente-se a esse conceito, a necessidade de que essas ações sejam asseguradas ao longo do ciclo de vida dos dados, ou seja, desde a coleta até o descarte ou eliminação.

Decorrem desse conceito, três pilares sobre os quais está calcada a Segurança de Informação:

- **Confidencialidade:** o titular de dados escolhe com quem ele quer dividir suas informações e dados e quanto dessa informação quer compartilhar. Fora disso todas as demais informações e dados devem ser confidenciais, não acessíveis.
- **Integridade:** deve haver garantia que as informações e dados quando sejam compartilhados, permaneçam íntegros, sem adulteração.
- **Disponibilidade:** a origem e o destino devem estar disponíveis para o tráfego de informações e dados; de modo que o titular tenha acesso quando deles necessite.

Patrícia Peck Pinheiro ao tratar da Segurança de Informação também diz que a mesma "visa a três pontos: a) confidencialidade: a informação só deve ser acessada por quem de direito; b) integridade: evitar que dados sejam apagados ou alterados sem a devida autorização do proprietário; e c) disponibilidade: as informações devem sempre estar disponíveis para acesso"[2]. Já alguns autores, como Antônio Everardo Nunes da Silva, defendem o acréscimo de mais dois aspectos: a autenticidade e a legalidade[3].

Podemos assim adicionar mais duas características: a Autenticidade, no sentido de que as informações e dados devem ser autênticos, sem adulteração; e a Legalidade, uma vez que a matéria é objeto de regulamentação.

Esses conceitos devem estar sempre em mira, haja vista que vão servir de base para toda e qualquer avaliação que se faça em termos de segurança de informação.

Ainda, aponte-se que a base legislativa da gestão da segurança de informação está no Marco Civil da Internet e no Decreto sob nº 8.771/2016.

O Marco Civil da Internet (MCI) – Lei nº 12.965/2014[4] estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil, os quais devem ser observados pelos entes federativos, provedores, empresas e todos aqueles que estão sujeitos ao trafego de informações e dados na rede mundial de computadores. Bruno Ricardo Bioni, ao mencionar o MCI explica que este:

> procurou, de forma principiológica, assegurar os direitos e garantias do cidadão no ambiente eletrônico, sendo o seu traço marcante a distância de uma técnica normativa prescritiva e restritiva das liberdades individuais, própria do âmbito criminal, que poderia ter efeitos inibitórios para a inovação e a dinamicidade da Internet[5].

A lei do MCI foi posteriormente regulamentada pelo Decreto nº 8.771/2016[6], especificamente para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicação, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações.

Com a edição da Lei Geral de Proteção de Dados Pessoais – Lei nº 13.709, de 14 de agosto de 2018[7], a segurança de informação ganhou melhores contornos, com o capítulo DA SEGURANÇA E DAS BOAS PRÁTICAS estabelecendo em seu artigo 46:

> Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

O § 2º do artigo 46, estabelece que "as medidas de que trata o *caput* deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução".

Do artigo 46 e seus parágrafos até o artigo 49 da LGPD, verificam-se alguns pontos que devem estar sempre em apreciação:

Medidas:

- de segurança
- técnicas
- administrativas
- desde a concepção > privacy by design

Proteção:

- acessos e comunicações não autorizados
- situações acidentais
- destruição, perda, alteração
- tratamento inadequado ou ilícito

Comunicações:

- agentes de tratamento
- titular de dados
- Autoridade Nacional de Proteção de Dados (ANPD)

Contudo, apesar da regulamentação prevista nas legislações citadas e das medidas de segurança que o legislador determina sejam adotadas, a possibilidade de ocorrerem violações, hackeamentos, vazamentos, jamais será totalmente descartada.

Objetiva-se portanto, destacar alguns cuidados considerados básicos para o exercício da segurança de informação no dia a dia, até porque conforme ensina Antônio Everardo Nunes da Silva[8], a maior causa de violações decorre de falha humana.

Disso se constata que depende de nós, titulares de dados, a responsabilidade pelo cuidado com as informações e dados, assim como segurança destes. Tanto no que diz respeito ao tratamento pessoal que damos a eles, como também no seu uso em ambientes corporativos, até porque em qualquer dessas situações são suscetíveis de vazamentos e violações.

Destacam-se como cuidados quanto à Proteção Pessoal:

- **Senhas fortes.** Usar senhas longas com diferentes tipos de caracteres, ex: letra maiúscula, minúscula, símbolos, números. Não usar teclas sequencias, nomes, datas ou dados.
- **Segundo Fator de Autenticação (2FA).** Método de segurança de gerenciamento de identidade e de acessos que exige duas formas de identificação para acessar recursos, aplicações e dados. Pode ser realizado por SMS, por e-mail, por token, por aplicativo autenticador.
- **Uma senha forte para cada aplicação.** Não utilizar a mesma senha para todas as aplicações, aplicativos, plataformas, etc. A variação no uso de senhas destina-se a limitar os riscos em caso da ocorrência de acesso indevido ou indesejado. Para tanto, recomenda-se o uso do gerenciador de senhas.
- **Gerenciador pessoal de senhas.** Aplicação de software que facilita a gestão das diversas contas e suas senhas, mediante o uso da criptografia. Há diversos gerenciadores, como por exemplo, NordPass, KeePass, 1Password, Keeper. Alguns gratuitos, outros pagos.
- **Backup de seus aparelhos pessoais em unidades externas criptografadas ou em nuvem.** O backup é uma cópia de segurança, que deve ser feita também para aparelhos pessoais, como celulares e tablets. Incluem-se serviços como Google Drive, ICloud, OneDrive, Dropbox, entre outros. Alguns gratuitos, outros pagos.
- **Rede doméstica segura e cuidado no uso em locais públicos.** Deve-se

partir do princípio de que redes públicas não são confiáveis. Há redes falsas e adredemente preparadas para a realização de golpes. Na dúvida, usar apenas a rede de dados móveis.

- **Contas do sistema operacional com menor privilégio.** Usar contas secundárias para os acessos diários e rotineiros. Não usar conta administrador para tudo. Não usar contas de convidado.
- **IMEI do aparelho celular.** Manter a anotação do IMEI do aparelho móvel, o que pode facilitar e agilizar as medidas de bloqueio, em caso de roubo ou uso indevido e inclusive, para fins de localização do aparelho.

Ainda, devido ao habitual envolvimento com trabalho, estudos e funções, destacam-se alguns cuidados quanto à Proteção em Ambiente Corporativo:

- **Equipe ou profissional de TI**. Manter um profissional e/ou equipe capacitados é absolutamente necessário em qualquer ambiente profissional. A prevenção, a orientação prévia, a avaliação da necessidade de cada negócio, assim como a implementação de adequados meios de segurança são medidas que devem ser realizadas com a atuação de profissionais técnicos e capacitados.
- **Criptografia.** Método de codificação de dados que permite o acesso apenas por pessoas autorizadas, portadoras de chave de acesso. Protege a integridade e o sigilo das informações e dados.
- **Firewall.** Recurso de software ou hardware que funciona como proteção, filtrando as informações que chegam e saem de uma rede. Serve como controlador do tráfego de uma rede privada.
- **Observação do princípio do menor privilégio**. Estratégia de administração de acessos e autorizações segundo as necessidades de cada atividade específica e de cada usuário. Trata-se de segmentação visando garantir que usuários acessem e utilizem apenas as informações e dados que sejam necessários para sua função ou atividade, isto é, de forma granular.
- **Senhas fortes**. Além da criação de senhas longas com diferentes tipos de caracteres, como já sinalizado em proteção pessoal, alterar as senhas constantemente, sem o uso de números sequencias (ex: senha001, senha002, senha003). Todas as contas de acesso devem ter senhas fortes e individuais. Não autorizar a memorização de senhas para fim de utilização automática e muito menos a troca de senhas ou o uso comunitário de alguma senha.

- **Segundo Fator de Autenticação (2FA) e Gerenciador de senhas**. O mesmo cuidado já tratado anteriormente quando da proteção pessoal aplica-se também para o ambiente corporativo, de modo a atribuir maior segurança ao uso das senhas. Há métodos e soluções especialmente desenvolvidos para o uso em empresas, como por exemplo: biometria, QRcode, certificado digital, Dashlane, RoboForm, Passwordstate, CyberArk.
- **Backup em fita, disco, nuvem, espelhamento**. Parafraseando a charada: quem tem dois, tem 1; quem tem 1, não tem nenhum. A utilização de rotinas de backup de informações e dados deve ser periódica, sendo que a escolha da melhor forma vai depender da necessidade, do tamanho, da área de atuação. Cada ambiente tem a sua necessidade. Cada negócio também.
- **Sistemas atualizados** em suas versões mais recentes, as quais possuem correções de falhas e vulnerabilidades, tornando-se menos suscetíveis a violações.
- **Software com assinatura, originais, licenciados**. Não permitir a instalação de programas não originais. Reproduções piratas além de violarem direitos autorais e se constituírem em crime digital, são mais suscetíveis a ameaças e violações.
- **VPN**. Trata-se de Rede Privada Virtual e corresponde a uma rede protegida para uso em rede de internet pública. Cria uma espécie de túnel entre uma máquina e a internet.
- **Confiança zero**. Trata-se de estratégia de segurança, que deve pautar os processos internos partindo da premissa de que nenhum usuário pode ser considerado confiável, até que tenha seus acessos autorizados e/ou validados. O conceito de Confiança Zero (*Zero Trust*) foi criado por John Kindervag[9], durante sua gestão como vice-presidente da Forrester Research, com base na percepção de que os modelos de segurança tradicionais operavam com base no pressuposto obsoleto de que tudo dentro da rede de uma organização deve ser confiável. Esse modelo trata a confiança como vulnerabilidade.
- **Gestão de identidades**. Trata-se da organização das identidades e acessos, categorizando as atribuições, papéis e responsabilidades, com a criação de perfis, de acordo com cargos e funções. É muito comum manter-se ativos perfis de colaboradores já desligados. Ou manter-se as credenciais de um colaborador mesmo após a sua mudança de função.

- **Conscientização** / treinamento de todos os funcionários e colaboradores, com especial atenção aos novos integrantes. Atualmente adota-se o processo de integração, que é uma das etapas mais importantes para novas contratações. Transmitir a estrutura, a cultura, os cuidados, os hábitos, estabelecer vínculos, são alguns dos benefícios dessa fase inicial da contratação e destina-se inclusive, para evitar as técnicas de engenharia social.

conclusão

Como conclusão, nunca é demais rememorar que embora todos nós tenhamos algum conhecimento acerca de cuidados com a segurança de informação, é extremamente necessário que haja o comprometimento pessoal, além do engajamento de equipes, colegas, colaboradores no âmbito corporativo, para o exercício efetivo de medidas de segurança e proteção, pois em geral os cibercriminosos esperam uma falha dos usuários e dos titulares de dados, para serem bem-sucedidos em suas constantes tentativas de ataque.

Aliado ao alerta feito por Bruno Ricardo Bioni na obra Proteção de Dados, contexto, narrativas e elementos fundantes, no sentido de que o país precisa da formação de uma cultura de proteção de dados pessoais, forçoso citar que o país precisa igualmente estabelecer e sedimentar uma cultura em segurança de informação.

notas de rodapé

1 Disponível em: <https://www.gov.br/gsi/pt-br/dsic/glossario-de-seguranca--da-informacao-1>. Acesso em: 05 nov. 2023.

2 PINHEIRO, Patrícia Peck. Direito Digital. 7ª. Edição, Editora Saraiva, 2021, pág. 223.

3 SILVA, Antônio Everardo Nunes da. Segurança da Informação, vazamento de informações. As informações estão realmente seguras em sua empresa?. 1ª Edição, Editora Ciência Moderna, 2012.

4 Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>.Acesso em: 05 nov. 2023.

5 BIONI, Bruno Ricardo. Proteção de Dados Pessoais A função e os limites do consentimento. 2ª. Edição, Editora Forense, 2020, pág. 124.

6 Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm>.Acesso em: 05 nov. 2023.

7 Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>.Acesso em: 05 nov. 2023.

8 SILVA, Antônio Everardo Nunes da. Segurança da Informação, vazamento de informações. As informações estão realmente seguras em sua empresa?. 1ª Edição, Editora Ciência Moderna, 2012.

9 Disponível em: <https://www.forrester.com/report/no-more-chewy--centers-the-zero-trust-model-of-information-security/RES56682?ref_search=3092262_1643722533656>.Acesso em: 05 nov. 2023.

Desafios, Estratégias e Procedimentos Práticos para Proteção dos Dados, Segurança das Informações

Thúlio Silveira

Projetos de adequação a Lei Geral de Proteção de dados (LGPD) podem durar anos, os desafios nesse período variam de acordo com as particularidades de cada empresa, diante disso é essencial a construção de conjuntos normativos e procedimentos internos, que possam servir como gatilhos para que as áreas estejam atentas a proteção de dados e segurança das informações.

1 analogia do alfaiate

Analisar seguimentos de mercado, operacionalizações, áreas da empresa, é primordial para entender o tamanho do desafio, quanto maior as variedades de operacionalizações, mais complexo o contexto para se criar mecanismos que atendam garantias necessárias, outro grande desafio é a necessidade de diversificação da abordagem com as diferentes áreas para que a cultura de segurança e privacidade seja efetiva.

2 privacidade e proteção de dados x segurança da informação

Infelizmente muitas vezes a devida importância a boas práticas e regulamentações vem precedido

por escanda-los causadores de impactos que fazem com que as organizações, repensem suas ações buscando garantias de que o mesmo não irá se repetir.

Para a Segurança das Informações a Lei americana Sarbanes-Oxley (SOx) de 2002 é considerada um marco visando proteger investidores de práticas fraudulentas, esta Lei foi precedida por escândalos que atingiram grandes empresas como Xerox e Enron (CAMARGO, 2017). Outras normas e padrões que mudaram a forma como as organizações tratam o tema são a norma ISO/IEC 17799 de 2000, o NIST Framework em 2014 e no Brasil em 2018 a resolução do BACEN nº 4658.

Para a proteção de dados pessoais, apesar de já existirem regimes individuais equacionadores como o código de defesa do consumidor, a devida importância sobre o tema só se materializou após a entrada em vigor do Regulamento Geral de Proteção de Dados (RGPD) em 2018 na Europa, impulsionado por escândalos como o uso dos dados pessoais de eleitores pela Cambridge Analytica, o que fez com que outras nações também dessem maior relevância ao tema.

3 **convergência**

As regulamentações relacionadas a Segurança da Informação, apesar de efetivas, não se aplicam ao contexto de todas as organizações, a adoção de medidas para muitas empresas ainda era subjetiva antes das Leis de Proteção de Dados, por exemplo a SOx é aplicável apenas as empresas de capital aberto.

As regulamentações sobre Proteção de Dados trouxeram convergência entre as duas matérias, se por um lado as regulamentações de segurança não eram impositivas a todas as empresas, a LGPD colocou todas no mesmo barco, e quando para garantir a Proteção dos Dados, é preciso medidas técnicas de segurança efetivas, automaticamente as organizações passam a proteger as duas matérias, por se tratar dos mesmos ativos envolvidos, nesse ponto os padrões internacionais como as ISOs da família 27000 se tornam relevante para todos os contextos.

4 **procedimentos práticos**

4.1 **estruturação de políticas internas e o apoio da alta direção**

A ISO 27002 prevê a estruturação de políticas de segurança, na LGPD é dito que os agentes devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais, pode-se dizer que é impossível a adoção de medidas sem uma política de privacidade e segurança que direcionem às pessoas através de diretrizes que atendam a necessidade de proteção das informações corporativas e dados pessoais.

Como na analogia do alfaiate, é preciso uma análise aprofundada sobre cada stakeholder para estruturar um grupo que fará a construção das diretrizes, garantindo um comitê multidisciplinar que observará as particularidades de todas as áreas. Outro ponto crucial é a representação da alta direção nesse grupo, para assegurar uma visão transparente das decisões, de forma hierárquica, partindo de cima pra baixo.

4.2 classificação das informações e princípios da LGPD

Não possível proteger o que não se sabe o valor, de acordo com a ISO 27002 convém que as informações sejam classificadas indicando a necessidade e o nível esperado de proteção, em paralelo a LGPD diz que os tratamentos de dados pessoais devem observar entre outros princípios a necessidade, segurança e prevenção.

Além da política de segurança, é importante criar diretrizes para classificar os dados em níveis adequados, identificando-os pelo menos em quatro níveis, público, interno, restrito e confidencial. Uma estratégia que pode ser adotada para que o mesmo instrumento contemple a classificação de dados corporativos e os dados pessoais é inserir os dados pessoais no penúltimo grau de criticidade, por exemplo restritos, e os dados pessoais sensíveis no ultimo grau de criticidade, dados confidenciais.

Outra estratégia que pode ser adotada para apoiar a assimilação a cultura é incluir a obrigatoriedade junto a outros processos, por exemplo no processo de formalização de documentos, pode ser alinhado junto a área responsável pelas revisões e publicações, a cobrança do responsável pelo documento para que o mesmo inclua o grau de sigilo das informações presentes, o que não substitui a necessidade da conscientização constante.

4.3 controle de acesso e princípio da segurança

Da mesma forma que é preciso saber o valor da informação, é preciso saber em quais ativos estão as informações relevantes para estabelecer medidas de controle de acesso, a ISO 27002 traz que convêm que recursos de processamento e processos de negócio sejam controlados, em paralelo na LGPD, temos o princípio da segurança que versa sobre a necessidade de medidas aptas a proteger dados pessoais de acesso não autorizado.

Nem sempre é possível automatizar o controle e revogações de acesso para todos os ativos, pois os dados podem estar espalhados por vários ambientes diferentes, por exemplo, sistemas internos, computadores, redes sociais, informação escrita, entre outros.

Para garantir esse controle e revogações, o primeiro ponto é identificar os equipamentos e sistemas utilizados, através da construção de inventários, identificando o responsável, a forma de acesso, os administradores, se o acesso é compartilhado e se é um ativo crítico para a informação, ou seja, se contém dados pessoais ou corporativos.

O segundo ponto é estabelecer junto aos gestores, uma comunicação com o responsável pela Proteção de Dados sempre que houver desligamentos, transferências de pessoal e termino de parcerias, para que os inventários possam ser consultados identificando quais são os acessos e direcionado as revogações pertinentes aos administradores de sistemas ou responsáveis pelos ativos.

4.4 processo de compra, contratação de serviços e a privacidade desde a concepção

A LGPD menciona que medidas de segurança, técnicas e administrativas para proteção de dados pessoais devem ser observadas desde a fase de concepção, em paralelo a ISO 27002 traz a previsão de que convém que acordos de segurança sejam estabelecidos para que as entregas atendam aos requisitos acordados.

Buscar processos que vinculem a análise da proteção dos dados em contratos previamente, incluindo o responsável pela proteção de dados nas análises, dentro de um fluxo padrão de compras, é uma estratégia para que as contratações sempre nasçam com os requisitos de segurança e proteção de dados necessários.

Na fase de solicitação de compras, pode-se alinhar para que o solicitante evidencie se a contratação tratará dados pessoais ou informações corporativas, para que exista uma avaliação prévia das intenções, antes mesmo da análise contratual, principalmente se a contratação envolver testes ou levantamentos pré-contratuais que tratem informações nessa fase, para que mesmo sem contrato estabelecido durantes testes ou levantamentos, sejam realizados dentro dos acordos de confidencialidade.

5 **conclusão**

Diante dos diversos desafios para implementação da proteção de dados nos processos internos, respeitando as particularidades de cada organização, uma abordagem integrada entre as recentes regulamentações relacionadas a proteção de dados e instrumentos já estabelecidos para segurança da informação é de extrema relevância, como legislações internacionais, setoriais, conjuntos normativos e padrões. A interpretação convergente e complementar dessas regulamentações e instrumentos, como os princípios da lei geral de proteção de dados em conjunto aos padrões e normas certificadoras de segurança da informação, pode auxiliar na construção de medidas práticas efetivas para proteção das informações e conformidade legal.

Além disso uma estratégia eficaz para apoiar a incorporação da cultura de segurança e privacidade nas organizações é a inclusão da alta direção para assegurar uma visão transparente e hierárquica das implementações, juntamente como a participação de membros multidisciplinares que possuam conhecimento aprofundado dos processos, ao estabelecer medidas a servir de gatilhos de atenção a segurança das informações e privacidade às pessoas envolvidas na execução dos processos.

Em conjunto, todas essas medidas não apenas podem ajudar a garantir a conformidade legal, mas também promover efetivamente a proteção das informações corporativas e dados pessoais.

referências bibliográficas

CAMARGO, Renata Freitas de. **Lei Sarbanes-Oxley (SOX):** O que é e como impacta as empresas. Treasy Blog, 22 de maio de 2017. Disponível em: https://www.treasy.com.br/blog/sox-lei-sarbanes-oxley/. Acesso em: 06 de novembro de 2023.

CONSELHO FEDERAL DE ADMINISTRAÇÃO (CFA). De onde veio a LGPD? Disponível em: https://cfa.org.br/de-onde-veio-a-lgpd/. Acesso em: 06 de novembro de 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 16 de novembro de 2023.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). NBR **ISO/IEC 17799:2005** - Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação. 2005. Disponível em: https://www.facom.ufu.br/~william/Disciplinas%202012-2/BSI%20-%20Auditoria%20e%20Seguranca/Material%20Adicional/NBR%20ISO-IEC%2017799-2005-PORTUGUES.pdf. Acesso em: 16 de novembro de 2023.

Gestão de incidentes de segurança e a importância da comunicação transparente em uma estrutura corporativa de proteção de dados

Fernando Vasconcelos

1 introdução

Falar em incidentes de segurança em um contexto de Lei Geral de Proteção de Dados nos leva, quase que automaticamente, a imaginar um cenário catastrófico de vazamento de senhas, ataques virtuais de hackers com toucas pretas em um quarto escuro e alguns outros clichês incentivados por cenas de filmes e séries.

Não que isso não exista ou que seja uma completa inverdade, mas a verdade é que falar em incidentes de segurança no contexto de dados e informações, é muito mais do que apenas isso. As possibilidades de vazamentos são muitas e, na maioria das vezes, são muito menos cinematográficas e muito mais ligadas às atividades do dia a dia do que podemos imaginar.

Um link clicado na hora errada, uma planilha enviada para quem não deveria receber, uma falta de comunicação entre áreas de uma mesma empresa, uma reunião com mais participantes do que os que realmente deveriam participar, enfim, todas essas atividades podem ser a origem, ou ao menos uma causa, de um incidente de segurança. Saber como lidar com casos como esses é o grande desafio dessa matéria.

Neste artigo não terei a pretensão de trazer um

extenso arcabouço técnico sobre o tema, até porque acredito que existam muitos outros acadêmicos e professores da área com maior capacidade para abordar o tema por esse viés. Me concentrarei em trazer, com esforços de usar uma linguagem acessível, as minhas experiências práticas do dia a dia de quem trabalha com proteção de dados desde o dia zero dentro de uma empresa de tecnologia.

2 **desenvolvimento**

Primeiramente, antes de qualquer coisa, o time ou o indivíduo carreira solo responsável pela proteção de dados de qualquer ambiente, deve se preocupar em criar ferramentas efetivas para que ele seja comunicado pela ocorrência de um incidente de segurança.

Ou seja, é fundamental que ele busque ferramentas para que as pessoas relacionadas, sejam elas colaboradores da empresa, fornecedores ou clientes, consigam comunicar a ocorrência de incidentes de segurança. E não são poucas as formas de criar esse fluxo de comunicação, variando de um simples e-mail "DPO@empresa.com.br" até formas mais completas e que se encaixam em contextos mais maduros como Portais de Privacidade ou Canais de Denúncias que viabilizem comunicações sobre vazamentos de dados/informações.

O principal objetivo na construção desse fluxo de comunicação é entender onde estão os principais riscos da sua atividade ao trabalhar com dados e viabilizar uma forma de comunicação que atenda efetivamente todos aqueles perfis que poderão relatar algum incidente, desde os próprios titulares de dados até um colaborador de uma empresa fornecedora que perceba uma eventual falha.

Com um canal de comunicação criado, o primeiro passo está feito, afinal agora você possui uma ferramenta específica que conecta os incidentes de segurança com aquele que tem a responsabilidade de geri-los e encontrar a melhor solução possível (o encarregado de proteção de dados).

Assim sendo, é fundamental que a cultura de proteção de dados seja espalhada e difundida entre todos aqueles que possuem relação com a empresa através de treinamentos, comunicações diárias sobre o assunto, inclusão de cláusulas de proteção de dados em contratos, publicação de uma política de privacidade efetiva e acessível para todos interessados, dentre outras ações que, quando somadas, criam uma cultura de dados e segurança alinhados com os objetivos da empresa.

A partir desse momento, é hora de se atentar à como gerir um incidente de segurança desde sua primeira comunicação. Para isso é essencial que o encarregado pela segurança de dados esteja bastante confortável sobre posicionar a alta diretoria sobre o assunto e buscar auxílio das áreas envolvidas no incidente.

O apoio da alta diretoria como um todo é parte fundamental na gestão dos incidentes, em especial para que a tarefa de designar horas de trabalho de colaboradores para corrigir o problema seja uma tarefa simples e que não tome mais tempo do que o necessário, afinal, em um cenário de incidente de segurança, qualquer tempo é importante e desperdiçar muito tempo com planejamento e sem nenhuma ação prática pode custar caro posteriormente.

Na minha experiência particular, uma estrutura adotada e que ajudou muito nos incidentes que surgiram foi a criação de um Comitê de Privacidade, contando com participantes de diversas áreas da empresa e dedicado exclusivamente ao acompanhamento de questões de segurança da informação e privacidade.

Um Comitê constituído em um momento que podemos chamar de "calmaria", quando nenhum incidente estava em pauta, possibilita a criação de um regimento próprio e definições práticas sobre quando se reunir, sobre o que discutir e qual ação se espera de cada um dos membros participantes. Inclusive, considero esse surgimento antecipado do Comitê de Privacidade como um grande aliado para o time de proteção de dados e, sem dúvidas, incentivo essa prática sempre que possível - já sabendo que nem toda realidade vai nos permitir esse privilégio da calmaria.

Considerado todo esse contexto prévia de estrutura, é hora de nos atentarmos sobre a gestão da ocorrência de um incidente de segurança na prática, quando ele verdadeiramente ocorre e ações responsivas precisam ser tomadas.

De início, ao receber o comunicado do incidente, por menor que ele possa parecer, a primeira medida a ser adotada é olhar para aquele relato de forma séria e evitando vieses que possam atrapalhar uma verdadeira análise do problema. Evite ao máximo olhar para um incidente com uma primeira opinião já formada, busque olhar para o problema de forma isenta e convoque os responsáveis pelas áreas envolvidas para uma avaliação da extensão daquele relato, sejam essas pessoas, fornecedores, colaboradores ou mesmo terceiros relacionados.

Uma vez analisado o problema e, se de fato constatado um incidente de segurança, é essencial que se prepare, dentro do prazo legal de 3 (três) dias úteis, duas formas de comunicação: uma comunicação direcionada para a ANPD e para qualquer outra autoridade relacionada ao caso específico; e outra relacio-

nada aos titulares de dados afetados, se possível de forma individualizada e com o maior nível de detalhamento possível.

Nesses casos, a transparência é o maior aliado das equipes de proteção de dados. Entenda o problema a fundo, busque entender o real dimensionamento do incidente e comunique tudo de forma clara e sem exageros. Faça uma comunicação simples, objetiva e completa.

Feitas as comunicações necessárias, é hora de olhar para dentro de sua estrutura para definir um plano de ação sobre como e quando agir para solucionar o problema e, neste ponto, não cabe falarmos o que deve ou não ser feito, uma vez que vai variar muito de caso a caso e de empresa para empresa. O ponto essencial é que exista um planejamento para corrigir o problema e que esse planejamento seja de fato cumprido (de preferência no menor tempo possível).

Portanto, endereçando os pontos finais deste artigo, considero que gerir bem um incidente de segurança está muito mais relacionado ao que você faz antes de um incidente ocorrer do que com as suas ações pós incidente de segurança.

conclusão

Para concluir, deixo claro que não estou dizendo que as etapas de gestão do incidente de fato (comunicação às autoridades e titulares, além das ações de correção) são menos importantes. Essas etapas também são fundamentais, mas são etapas conclusivas de um processo; ou seja, elas só vão existir se a lição de casa tiver sido feita anteriormente.

Assim sendo, com base em minhas experiências de dia a dia, entendo que o grande ponto é que essas etapas só serão eficazes e produtivas se, antes de qualquer incidente, o seu time de proteção de dados tenha sido capaz de "preparar o terreno" internamente, especialmente no que se refere à criação de uma cultura presente de zelo e cuidado pelos dados pessoais e informações utilizadas pela companhia.

SEÇÃO V

Normas & Governança em Privacidade

Análise da norma ABNT NBR ISO/IEC 29151 e seus benefícios para Programas de Governança em Privacidade

Bruna Cruz

1 introdução

Na sociedade atual a informação é o seu novo elemento estruturante, vez que ela passou a representar um papel de destaque, ao ponto de transformar completamente o padrão em que se estruturam as relações sociais. Assim, na sociedade da informação, os dados se tornaram os ativos com maior valor econômico, transformando-se na moeda de troca mais preciosa do mercado, tanto que passou a ser denominada como o novo petróleo. Entretanto, não é a informação em si que aumenta a eficiência da atividade empresarial, mas seu processo de organização, o qual será´ transformado em conhecimento aplicado. (BIONI, 2020).

Desse modo, o tratamento dos nossos dados pessoais vem mudando o formato da economia, vez que as informações sobre os nossos hábitos de consumo dão permissão para que as empresas possam empreender de maneira mais eficiente no mercado, aumentando o êxito nas vendas e melhorando a forma como o produto é vendido. Assim, observa-se a importância dos dados pessoais no cenário mundial, que passaram a assumir um protagonismo, a ponto de criar uma completa alteração nos padrões nos quais estão inseridas as relações comerciais e estruturais.

A tecnologia e as mudanças sociais definem um

novo cenário global, em que a privacidade e a informação pessoal se entrecruzam, passando a primeira, a se estruturar por meio da segunda, principalmente no que concerne aos dados pessoais. (ARAÚJO; CAVALHEIRO, 2014)

Nesse contexto, todavia, surge um grande problema, pois parte da população mundial não tem ideia de que diariamente está sendo monitorada por meio de apenas um clique ou que seus dados pessoais estão sendo vendidos, sem que se tenha conhecimento: como nos casos dos "profiling" (análises comportamentais), dos algoritmos para tomadas de decisão e da venda de bancos de dados.

Sistemas eletrônicos constantemente produzem uma grande quantidade de dados, criando pontos de comunicação entre o mundo físico e virtual. Transações comerciais, relações sociais eletrônicas, ou até´mesmo o ato de andar pela rua (dados de geolocalização utilizados pelos "smartphones") geram um fluxo gigantesco de dados pessoais, que, constantemente, são tratados em consonância com a vida cotidiana em sociedade. (CARVALHO, 2019)

Observando-se esse tratamento desenfreado de dados pessoais, que na maioria das vezes gerava riscos à privacidade do titular, surge a necessidade de criação de um regulamento que protegesse os dados pessoais no mundo interconectado em que vivemos. Sendo assim, em setembro de 2020, entrou em vigor a Lei Geral de Proteção de Dados [LGPD].

No entanto, apenas a análise da nova legislação é insuficiente para criar padrões técnicos de privacidade e de segurança da informação suficientes para que as empresas sejam capazes de criar um Programa de Gerenciamento de Privacidade robusto e adequado às boas práticas do mercado internacional.

Assim, recorre-se aos padrões internacionais, como os das normas ditadas na Associação Brasileira de Normas e Técnicas [ABNT] (Foro Nacional de Normalização) que é uma entidade privada sem fins lucrativos, fundadora da Organização Internacional de Normalização [ISO]. Os processos de normatização contidos na ABNT NBR ISO/IEC se dão por meio da aplicação das regras contidas em um documento padrão, cujo objetivo é facilitar as transações comerciais, fomentar o avanço tecnológico e a promoção das boas práticas de gestão, as quais têm como premissa previr e solucionar problemas.

A escolha da presente temática se deu em virtude da necessidade da aplicação de um "Framework" robusto, além de adequado às normas e aos padrões internacionais no que concerne à privacidade e à segurança da informação. Com isso, as empresas poderão utilizar, na nova realidade, essas diretrizes de adaptação de maneira assertiva e eficaz, por meio da aplicação da norma ABNT NBR ISO/IEC 29151 - Tecnologia da informação - Técnicas de segurança - Código de

prática para proteção de dados pessoais, que fornece uma metodologia segura e eficiente.

2 conceito de um programa de gerenciamento em privacidade

Cotidianamente escuta-se diversas notícias de incidentes de segurança e privacidade nas organizações, o que acarreta a incidência de multas e aumenta o risco tanto para os titulares de dados, quanto para os demais "stakeholders" envolvidos com a organização. Em 2020, a Lei Geral de Proteção de Dados (lei nº 13.709) entrou em nosso ordenamento jurídico com o intuito de trazer uma maior segurança para as empresas e para os cidadãos detentores de dados pessoais. Ressalte-se que decidissem utilizar as medidas de prevenção, consequentemente, ganhariam uma vantagem competitiva sobre àquelas que não tivessem esse tipo de preocupação.

Todavia, consoante Viviane Maldonado (2019), apenas a LGPD, a partir da sua compreensão meramente teórica, é incapaz de assegurar a proteção dos dados pessoais, vez que para a lei atingir sua finalidade específica, deve ser implementada na prática, pois o alcance dos fins buscados por meio da eficácia da adequação, deve ser acompanhado de controles robustos de segurança da informação, os quais devem estar dispostos ao longo de todo o processo de conformidades, desde suas fases iniciais.

Quando se observa a lei, no intuito de encontrar diretrizes que se adequem a realidade das empresas, o seu art. 50, apresenta uma redação vaga, sem de fato explicar quais controles devem ser implementados. Observa-se:

> Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

Para que a matéria jurídica se torne uma realidade prática, deve-se criar dentro das organizações um Programa de Governança em Privacidade, que nada mais é que uma abordagem construída internamente, cujo objetivo se traduz em juntar diversas diretrizes e padrões dentro de um "framework "(estrutura) que permita que uma organização atenda aos requisitos de privacidade e segurança da informação no dia a dia da empresa. (IAPP, 2020) Tais diretrizes proporcionam uma segurança mais eficaz tanto para as empresas, quanto para os seus consumidores, uma vez que diminuem o nível de risco de uma violação de dados pessoais.

A expressão "framework" é largamente utilizada em diversos modelos, processos, metodologias, ferramentas e padrões que podem orientar profissionais a criar uma metodologia para vários temas. No que tange à privacidade, os "frameworks" surgiram nos anos 70 com o intuito de orientar profissionais, consultorias e organizações a criar um programa robusto no gerenciamento de privacidade e segurança da informação. (IAPP, 2020)

Além do "framework" escolhido, um Programa de Governança em privacidade holístico e robusto, deve identificar no mínimo: as obrigações de privacidade da empresa; os riscos de privacidade da atividade dos clientes e dos funcionários; informações pessoais coletadas e tratadas; e criar, bem como implementar políticas, processos e procedimentos existentes. Ressalte-se, também, a importância de se criar metas tais como: melhorar a reputação da empresa; promover a confiança dos clientes e investidores; responder às violações de segurança e privacidade; conscientizar seus colaboradores frente às novas obrigações; e monitorar, bem como melhorar continuamente o programa. (IAPP, 2020)

Sendo assim, anseia-se pela criação de um programa robusto apto a proteger o cidadão, e, que consequentemente, demonstrará a responsabilidade da empresa na proteção dos dados pessoais e nos ativos da organização, gerando assim, um maior grau de segurança e confiança em todos os "stakeholders" envolvidos.

3 **principais frameworks de privacidade do mercado**

Mercadologicamente, observou-se que empresas que estejam adequadas às boas práticas de segurança da informação e privacidade dispõem de um diferencial competitivo em relação às demais, situação que desencadeia uma busca de metodologias robustas internacionais e nacionais, para que as empresas co-

meçassem de forma segura os seus projetos de adequação à LGPD.

Por meio da pesquisa de mercado, verificou-se a existência de diversos "frameworks", alguns mais voltados para a gestão da segurança da informação, para diretrizes de privacidade, e para ambos. Da mesma forma, foram constatadas metodologias voltadas para os setores específicos de negócio, bem como para pequenas e médias empresas.

Nesse contexto, a primeira norma destacada é a ABNT NBR ISO/IEC 27001 (Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos), um padrão internacional voltado para gestão da segurança da informação, que tem como finalidade identificar, analisar e implementar, dentro da organização, controles para avaliar, analisar, implementar, gerenciar e mensurar os riscos de segurança da informação, assim como proteger a integridade, a confidencialidade e a disponibilidade dos dados internos.

Outros "frameworks" que merecem destaque foram publicados pelo "National Institute of Standards and Technologies"- NIST. O primeiro deles está voltado para controles de SI, e se denomina "Framework for Improving Critical Infrastructure Cybersecurity", o qual permite que organizações, sem embargo do seu tamanho ou grau de risco, possam aplicar as melhores práticas voltadas para o gerenciamento de riscos, por meio de múltiplas estratégias de segurança cibernética. O segundo é o "An Introduction to Privacy Engineering and Risk Manegement" publicado com o intuito de introduzir definições sobre engenharia de privacidade e gestão de risco para sistemas federais. (IAPP, 2020)

Outra metodologia que vale a pena ser destacada é o"Health Insurance Portability and Accountability Act [HIPAA]", uma legislação promulgada nos Estados Unidos que foi criada para regular nacionalmente os padrões de transações eletrônicas na área da saúde, além de proteger a privacidade e segurança dos dados desta área. (IAPP, 2020)

Destacando-se as metodologias nacionais, a primeira que se deve mencionar é o "Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte", publicado pela Autoridade Nacional de Proteção de Dados, cujo intuito é endereçar boas práticas para empresas de pequeno porte, dentre as quais, as que, em razão do tamanho possuem limitações, e, assim, são indicadas diretrizes de segurança da informação para proteger os dados pessoais que estão sob sua guarda. (ANPD, 2021)

O pioneiro dos "frameworks" publicados por órgãos nacionais, é o "Guia de Avaliação de Riscos de Segurança e Privacidade", divulgado pelo Governo Digi-

tal (Ministério da Economia), fornece as entidades públicas orientações sobre análise de risco e um questionário composto por 113 controles que auxiliam na identificação de lacunas de privacidade e segurança da informação nos seus processos, contratos e sistemas. (Governo Digital, 2020)

E, por fim, destaca-se a norma ABNT NBR ISO/IEC 29151 (Tecnologia da informação - Técnicas de segurança - Código de prática para proteção de dados pessoais), que é considerada a mais completa do mercado tanto nacional, quanto internacional, a qual será analisada com maior profundidade no próximo tópico.

4 principais aspectos analisados em uma empresa a partir das diretrizes da norma ABNT ISO/IEC 29151

O "*framework*" da norma ABNT NBR ISO/IEC 29151 (Tecnologia da informação - Técnicas de segurança - Código de prática para proteção de dados pessoais) é um documento que fornece diversas orientações aos agentes de tratamento. Nele, utiliza-se um extenso rol de conceitos, bem como controles de privacidade e segurança da informação, os quais podem ser adaptados e aplicados a qualquer tipo e tamanho de organização, suplementando os controles contidos na ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002.

Com o objetivo de criar um Programa de Gerenciamento em Privacidade robusto, o padrão internacional explicita diversas nuances que precisam ser criadas, implementadas e revisadas dentro dos processos das empresas, além de auxiliá-las a definir quais ações e prioridades são mais adequadas para gerenciar os riscos e os tratamentos na proteção dos dados pessoais.

A escolha dos controles que serão aplicados sujeita-se às decisões das empresas, que terão como base os parâmetros escolhidos para o tratamento e a gestão dos seus riscos internos. Esses controles também serão aplicados de acordo com a atividade da organização, do fornecimento de infraestrutura ou dos serviços, por meio de acordos contratuais entre seus clientes e fornecedores. Também se faz necessário que a organização esteja sujeita a todas as leis e regulamentos aplicáveis à sua atividade. (ABNT NBR ISO/IEC 29151, 2020)

Dessa forma, a supracitada norma fornece os mais diversos controles para que possam ser adaptados a qualquer tipo de realidade, estando de acordo com a finalidade de cada tratamento em questão, desde relações trabalhistas até programas como o "*big data analytics*".

O primeiro controle indispensável que se observa, é a necessidade do mapeamento do ciclo de vida dos dados, obrigação que se encontra no art. 37 da LGPD. Destarte, observa-se que uma organização precisa ter registrado em seus documentos internos desde a coleta, tratamento, armazenamento até o descarte dos dados pessoais. (ABNT NBR ISO/IEC 29151, 2020)

Políticas de Segurança da Informação precisam estar implementadas e divulgadas, incluindo declarações pertinentes aos critérios necessários para proteção dos dados pessoais, evitando que este conteúdo esteja em um documento apartado. Além de políticas para uso de dispositivos móveis e para o trabalho remoto (quando necessário para a realidade da organização). (ABNT NBR ISO/IEC 29151, 2020)

Outro controle essencial é a necessidade de definição dos papéis e das responsabilidades de forma clara, a partir da criação de um comitê multidisciplinar, portado de autonomia e independência, e que auxilie na identificação de riscos e oportunidades de melhoria. Também convém que seja designado um indivíduo sênior, que avoque a responsabilidade pelo gerenciamento da proteção de dados internamente, denominado pela LGPD no art. 5º, VIII de encarregado, que seria o ponto de contato interno entre os titulares e as autoridades para direcionar questões relativas ao tema. (ABNT NBR ISO/IEC 29151, 2020)

Torna-se primordial, além dos treinamentos de segurança da informação, a criação e implementação de diretrizes para conscientizar os colaboradores das mais diversas áreas acerca dos procedimentos internos de privacidade e das possíveis consequências em violar as regras de privacidade (consequências legais, processos disciplinares, danos de reputação ou perda de negócios). (ABNT NBR ISO/IEC 29151, 2020)

Cumpre destacar que um dos principais pontos relacionados à segurança cibernética da empresa é a sua gestão de ativos, que deve ser feita por meio de diversos controles, tais como: inventários de “software”e“hardware”, classificação da informação e gerenciamento de mídias físicas (controle, descarte e transferência). (ABNT NBR ISO/IEC 29151, 2020)

As empresas também devem verificar os procedimentos para registro e cancelamento dos usuários, utilizando-se do seu controle de acesso e por meio de medidas que solucionem riscos, como por exemplo, comprometimento de senhas, alterações indevidas e divulgação inadvertida. Portanto, compete às organizações restringirem o acesso aos sistemas que tratem de dados pessoais apenas aos usuários necessários para a operação, além da criação de métodos robustos de “log-in” e autenticação. (ABNT NBR ISO/IEC 29151, 2020)

Outro ponto essencial é a segurança física do ambiente. Neste quesito, as empresas devem se preocupar tanto com as áreas onde estão sediados seus equipamentos, quanto a segurança dos próprios equipamentos em si. Com isso, a empresa deve se atentar à manutenção e ao descarte seguro dos equipamentos, à segurança do cabeamento, à remoção de ativos, à política da mesa limpa, etc. (ABNT NBR ISO/IEC 29151, 2020)

Além disso, a segurança nas operações é outro ponto destacado pela norma, como a gestão de mudanças, gestão da capacidade e da redundância, criação de cópias de segurança, proteção contra códigos maliciosos, registro de "*logs*", sincronização de relógios e gestão de vulnerabilidades. (ABNT NBR ISO/IEC 29151, 2020)

Convém também que sejam adotadas medidas apropriadas para reduzir o risco de vazamento de dados durante o compartilhamento ou transferência internacional das informações, tais como a anonimização, a pseudoanonimização, a criptografia ou por condições específicas sobre como e quais tratamento de dados externos de dados pessoais podem ocorrer (contratos ou acordo de processamento de dados). (ABNT NBR ISO/IEC 29151, 2020)

Outro ponto importante, segundo a ABNT, é o relacionamento da empresa com seus fornecedores, pois eles devem ser avaliados antes da contratação, com base na sua experiência, credibilidade e capacidade em atender aos requisitos da legislação. Além disso, é importante que se tenha um contrato por escrito delimitando os papéis e responsabilidades de cada agente, sem a permissão de subcontratação sem uma aprovação prévia e não permitindo que os dados sejam tratados para quaisquer outros fins que não estejam delimitados no contrato. (ABNT NBR ISO/IEC 29151, 2020)

Do mesmo modo, é de extrema relevância que a organização esteja capacitada para prover uma resposta eficaz e organizada a um incidente de privacidade ou segurança da informação, que contenha: definição do incidente e sua resposta; uma equipe multidisciplinar para gerenciar; processos internos para notificar colaboradores envolvidos; avaliação do impacto do incidente, a natureza e a extensão do dano; medidas mapeadas para mitigar os riscos; e procedimentos para fornecer notificação às autoridades e titulares envolvidos. (ABNT NBR ISO/IEC 29151, 2020)

E por fim, devem-se observar aspectos de gestão de continuidade de negócios, em que a empresa deve se planejar para que possa responder a falhas ou incidentes que causem interrupções nos seus negócios, para que suas operações continuem durante o evento, garantindo um nível adequado de segurança da informação. (ABNT NBR ISO/IEC 29151, 2020)

5 considerações finais

Mediante os estudos e pesquisas realizados, constatou-se que a Lei Geral de Proteção de Dados, comumente conhecida como LGPD, em sua compreensão puramente teórica é insuficiente para criar diretrizes e padrões seguros de privacidade e segurança da informação, capazes de criar um Programa de Gerenciamento em Privacidade robusto, que adeque as empresas às boas práticas do mercado internacional. Diante desse contexto, a pesquisa teve como objetivo geral analisar a norma ABNT NBR ISO/IEC 29151, em que se constatou a sua eficiência em definir quais controles são mais adequados para gerenciar os tratamentos e riscos na proteção dos dados pessoais, apresentando uma abordagem holística, a qual pode ser implementada na maioria das empresas atuantes no mercado, independente do porte, escopo ou do volume de dados. Assim, ao analisar as organizações por meio dos controles constantes na já citada metodologia, observa-se com maior assertividade os pontos internos que apresentavam maior fragilidade e que precisavam ser criados ou reajustados, bem como aqueles que já eram atendidos, trazendo uma maior eficácia para o ajuste dos seus processos e sistemas internos, além de trazer segurança para o que precisava de investimento.

O estudo também teve como objetivo analisar quais eram os principais "frameworks" utilizados no mercado, destacando-se: a norma ABNT NBR ISO/IEC 27001, o "*Framework for Improving Critical Infrastructure Cybersecurity*", o "*An Introduction to Privacy Engineering and Risk Management*" (ambos do NIST), o "*Health Insurance Portability and Accountability Act-HIPAA*", o Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte", o "Guia de Avaliação de Riscos de Segurança e Privacidade", e a norma ABNT NBR ISO/IEC 29151, dissertando sobre suas indicações e especificidades de acordo com o escopo de cada empresa e sobre suas fragilidades.

Analisou-se igualmente as principais diretrizes de proteção de dados que uma empresa deve observar contidadas na a norma ABNT NBR ISO/IEC 2915, atentando-se entre seus controles: a necessidade da criação de um Inventário de dados, a criação de políticas, canal de atendimento aos titulares, nomeação de um responsável pelo tema, definição dos papéis e responsabilidades das empresas, análise contratual, capacitação de seus colaboradores. Entre as melhores práticas de segurança da informação, tem-se: o gerenciamento de seus ativos, gerenciamento de seus usuários, segurança de dispositivos móveis, gestão de mudanças, capacidade e redundância, transmissão segura por meio de controles criptográficos, gestão de riscos e continuidade.

referências bibliográficas

ABNT. **Sobre a normalização**. Disponível em: <https://www.abnt.org.br/normalizacao/sobre>. Acesso em 16 Abr. 2022.

. **Institucional**. Disponível em: <https://www.abnt.org.br/institucional/sobre>. Acesso em 16 Abr. 2022.

ABNT NBR ISO/IEC 27001:2013: Tecnologia da informação — **Técnicas de segurança** — Sistemas de gestão da segurança da informação — Requisitos. Rio de Janeiro. Associação Brasileira De Normas Técnicas. 2013.

ABNT NBR ISO/IEC29151:2020: Tecnologia da informação - **Técnicas de segurança** - Código de prática para proteção de dados pessoais. Rio de Janeiro. Associação Brasileira De Normas Técnicas. 2020.

Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte [ANPD]. 2021. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e- publicacoes/guia-vf.pdf>. Acesso em 16 Abr. 2022.

BBC. **Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades**. G1. 2018. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml>. Acesso em 16 Abr. 2022.

Bioni, Bruno Ricardo. **Proteção de Dados Pessoais**, a Função e os Limites do Consentimento. 2. Ed. Rio de Janeiro: Editora Forense, 2020.

. **Inovar pela lei**. GV EXECUTIVO, v. 18, n. 4, p. 30-33, 2019.

. **Regulação de Dados é uma janela de oportunidade**. Data Privacy, 2019. Disponível em: <https://dataprivacy.com.br/regulacao-de-dados-e-uma-janela-de- oportunidade/>. Acesso em 16 Abr. 2022.

BRASIL, **LEI No 13.709, DE 14 DE AGOSTO DE 2018**. Lei Geral de Proteção de Dados (LGPD), Brasília, DF, dez 2018. Disponível em: <http://www.planalto.gov.

br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 15 Abr. 2022.

Carvalho, Luiz *et al*. **Desafios de Transparência pela Lei Geral de Proteção de Dados Pessoais**. *In:* Anais do VII Workshop de Transparência em Sistemas. SBC. p. 21-30. 2019.

Cots, Márcio. **Lei Geral de Proteção de Dados Pessoais, Comentada**. 1. Ed. São Paulo: Revista dos Tribunais. 2019.

Couto, Marta Lais dos Santos Alegria. **O e-commerce à luz do direito: análise do regulamento geral da proteção de dados**: a uniformização da União Europeia. Dissertação de Mestrado. Universidade Católica Portuguesa (UCP). 2016.

Araujo, Luiz Ernani Bonesso; CAVALHEIRO, Larissa Nunes. **A proteção de dados pessoais na sociedade informacional brasileira**: o direito fundamental a privacidade entre a autorregulação das empresas e a regulação protetiva do internauta. Revista do Direito Público, v. 9, n. 1, p. 209-226, 2014.

Menezes Neto, Elias Jacob; DE MORAIS, Jose Luis Bolzan; BEZERRA, Tiago José de Souza Lima. **O projeto de lei de proteção de dados pessoais (PL 5276/2016) no mundo do big data**: o fenômeno da dataveillance em relação à utilização de metadados e seu impacto nos direitos humanos. Revista Brasileira de Políticas-Públicas. v. 7, n. 3, p. 184-198. 2018.

DIGITAL, Governo. **Guia de Avaliação de Riscos de Segurança e Privacidade**. 2020. Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e--protecao-de- dados/guias/guia_avaliacao_riscos.pdf/view>. Acesso em 18 Abr. 2022.

Doneda, Danilo. **A proteção dos dados pessoais como um direito fundamental**. Espaço Jurídico Journal of Law [EJJL], v. 12, n. 2, p. 91-108.2011.

. **Da Privacidade à Proteção de Dados Pessoais, Elementos da Formação da Lei Geral de Proteção de Dados**. 2. Ed. São Paulo: Revista dos Tribunais. 2019.

Doneda Danilo; MENDES, Laura; BIONI, Bruno. **Tratado de Proteção de Dados Pessoais**. 1. Ed. Rio de Janeiro: Forense, 2021.

FLOWTI. **Como a Segurança da Informação é afetada pela nova Lei Geral de Proteção de Dados**. Disponível em: <https://flowti.com.br/blog/como-a-seguranca-da-informacao-e-afetada-pela-nova-lei-geral-de-protecao-de-dados>. Acesso em 19 Set. 2022.

Lima, Caio Cesar Carvalho; Monteiro Renato Leite. **Panorama brasileiro sobre a proteção de dados pessoais: discussão e análise comparada**. AtoZ: novas práticas em informação e conhecimento. v. 2, n. 1, p. 60-76. 2013.

Maldonado, Viviane Nóbrega; Blum, Renato Opice; Borelli, Alessandra. **Comentários ao GDPR**: regulamento geral de proteção de dados da União Europeia.2. Ed. São Paulo: Revista dos Tribunais. 2020.

Maldonado, Viviane Nóbrega; Blum. LGPD, **Lei Geral de Proteção de Dados Pessoais, Manual de Implementação**.1. Ed. São Paulo: Revista dos Tribunais. 2019.

Mulholland, Caitlin. Mangeth, Ana. **Análise Comparativa entre os Princípios Informadores do Regulamento Geral de Proteção de Dados da União Europeia e as Normas do Direito Brasileiro**. Puc-Rio. 2018.

Pscheidt, Kristian. **Lei de proteção de dados: importância e o impacto nas empresas**. Migalhas. 2018. Disponível em: <https://www.migalhas.com.br/depeso/286426/lei-de- protecao-de-dados-importancia-e-o-impacto-nas-empresas>. Acesso em 17 Abr. 2022.

As normas corporativas globais como mecanismo de comprovação de garantias nas transferências internacionais de dados pessoais

Fernanda Ratzkowski

1 introdução

O rápido avanço da tecnologia digital e a intensificação do processo de globalização têm provocado uma transformação profunda na forma como empresas e indivíduos compartilham dados em escala global. Esse dinâmico intercâmbio de informações é, indiscutivelmente, um alicerce vital para as transações comerciais, impulsionando não apenas a agilidade nas operações financeiras, mas também facilitando acordos comerciais internacionais e estimulando a inovação.

No entanto, apesar de proporcionar benefícios econômicos significativos, a expansão da conectividade global traz consigo desafios cruciais relacionados à segurança e proteção dos dados pessoais envolvidos nas transferências internacionais. Nesse cenário, regulamentações como a Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais ("LGPD") no Brasil e o Regulamento Geral sobre Proteção de Dados 2016/679 ("GDPR") na União Europeia desempenham um importante papel ao estabelecer normas e diretrizes que buscam garantir a segurança e a proteção desses dados.

Destarte, embora o Brasil tenha delineado meca-

nismos para as transferências internacionais de dados, ainda enfrenta desafios em sua plena regulamentação. Assim, o presente artigo busca suscitar reflexões sobre as lições que o país pode extrair da experiência europeia - com especial enfoque no mecanismo das normas corporativas globais - a fim de fortalecer ainda mais sua postura em relação à proteção de dados pessoais em um contexto globalizado.

2 as transferências internacionais de dados pessoais

A LGPD trata das transferências internacionais de dados pessoais em seu capítulo V, entre os artigos 33 e 36[1]. De forma análoga, o GDPR estabelece as disposições sobre as transferências internacionais no capítulo V, que vai do artigo 44 ao artigo 50[2].

Ambos os regulamentos estipulam que a transferência de dados pessoais para outros países pode ocorrer somente mediante uma decisão de adequação emitida pela autoridade responsável pela regulação da proteção de dados. Na ausência de tal decisão, os regulamentos fornecem orientações sobre os instrumentos legais apropriados. Da mesma forma que o GDPR no artigo 46[3], o legislador brasileiro previu, no artigo 33, II, da LGPD, mecanismos para "fornecer e demonstrar a conformidade com os princípios, os direitos do titular e o regime de proteção de dados estabelecidos"[4].

Diante desse cenário, vale ressaltar que a LGPD foi bastante influenciada pela lei europeia[5]. Isto é, o próprio parecer da Comissão Especial da Câmara dos Deputados, instituído para analisar o Projeto de Lei nº 4060/2012, estabeleceu que "grande fonte de inspiração para os projetos advém do arcabouço europeu"[6].

Contudo, muito embora a LGPD tenha estabelecido os mecanismos a serem utilizados para garantir os níveis adequados de segurança nas transferências internacionais de dados, tais instrumentos ainda pendem de regulamentação. Portanto, o Brasil encontra-se atualmente em um estágio menos avançado em relação à regulamentação dos mecanismos, quando comparado com a União Europeia.

Nesse contexto, a transferência internacional de dados pessoais foi incluída no item 9 da agenda regulatória bianual 2021-2022 da Autoridade Nacional de Proteção de Dados ("ANPD")[7]. Durante esse período, a ANPD conduziu um processo de consulta pública entre maio e junho de 2022, que resultou na recepção

de 63 contribuições[8].

Em agosto de 2023, uma nova consulta pública foi lançada com o objetivo de regulamentar as transferências internacionais de dados pessoais e apresentar um modelo de cláusulas-padrão contratuais[9]. A consulta pública permaneceu aberta por dois meses e recebeu um impressionante número de mais de duas mil contribuições[10].

3 as normas corporativas globais

Dentre os mecanismos de salvaguardas para transferências internacionais de dados trazidos pelos regulamentos brasileiro e europeu, destacam-se as normas corporativas globais. As normas corporativas globais compreendem códigos de conduta que definem as políticas internas aplicáveis às transferências de dados pessoais dentro das empresas[11], grupos corporativos, e grupos de empresas envolvidos em atividade econômica conjunta, como franquias, joint ventures ou parcerias profissionais[12].

Destarte, o mecanismo visa harmonizar as práticas entre as diferentes empresas ou sedes constituintes de um mesmo grupo, independentemente de sua localização ou da cidadania de seus funcionários[13]. Isso contribui de forma significativa para a mitigação dos riscos associados ao tratamento de dados pessoais, especialmente nas entidades localizadas em países desprovidos de bases normativas sólidas de proteção de dados[14].

A adoção das normas corporativas globais revela-se particularmente avançada no contexto europeu e sua regulamentação pelo órgão brasileiro pode representar um importante passo para o Brasil no que tange à garantia da conformidade, proteção e segurança dos dados pessoais. De fato, regulamentar as normas corporativas globais permitirá ao Brasil usufruir desse mecanismo, proporcionando maior agilidade e fluidez nas transferências internacionais de dados pessoais no âmbito interno das empresas multinacionais e grupos empresariais localizados no país.

Como se sabe, a LGPD pode se beneficiar da evolução legislativa do GDPR para incorporar seus elementos[15]. Desse modo, para uma compreensão mais aprofundada das normas corporativas globais, é relevante que se apresente, de maneira consolidada, a percepção e aplicação desse instrumento na União Europeia.

Nesse contexto, destaca-se a valiosa a contribuição do Grupo de Trabalho

do Artigo 29, - órgão consultivo independente formado pelos reguladores de proteção de dados dos Estados-membros da União Europeia - que adotou o documento "*Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers*"[16] em 3 de junho de 2003. Este documento fornece contribuições detalhadas sobre as normas corporativas globais, apresentando grande utilidade para as autoridades e agentes brasileiros que venham a utilizar este mecanismo.

Inicialmente, conforme destacado pelo Grupo, é fundamental que as normas corporativas globais abranjam os princípios dispostos na legislação europeia de proteção de dados[17]. Vale mencionar que tais princípios podem significar pouco para empresas e colaboradores que tratam dados fora da União Europeia[18]. Assim, é imprescindível que as solicitações para aprovação das normas corporativas globais contenham descrições minuciosas de informações como o fluxo de dados pessoais, as transferências autorizadas, os destinos dos dados e as finalidades do tratamento, a fim de que se verifique se, o tratamento realizado em países terceiros é compatível com os níveis de proteção de dados pessoais da União Europeia[19].

Além disso, o Grupo destaca que as normas corporativas devem ser, de fato, de caráter global - ou seja: aplicáveis ao grupo corporativo como um todo, independentemente do local de estabelecimento dos membros ou da nacionalidade das pessoas cujos dados pessoais estão sendo tratados[20].

No mais, as terminologias sugeridas pelo Grupo para definir o mecanismo são: "regras corporativas vinculantes para transferências internacionais de dados"[21] ou "regras corporativas legalmente exigíveis para transferências internacionais de dados". Essas normas podem ser caracterizadas da seguinte forma: (i) são vinculativas ou legalmente exigíveis, a fim de constituírem "garantias suficientes", e, portanto, legalmente executáveis; (ii) têm natureza corporativa, visto que se baseiam nas políticas em vigor nas empresas multinacionais, normalmente elaboradas sob a supervisão da matriz; e (iii) têm como principal finalidade a regulamentação de transferências internacionais de dados[22].

Vale dizer, a noção de grupo corporativo pode variar de um país para outro e pode corresponder a realidades de negócios muito diferentes[23]. Tais diferenças na estrutura e atividade impactam sobre a aplicabilidade, projeto e escopo das regras corporativas obrigatórias e grupos corporativos devem ter isto em mente ao apresentar suas propostas[24].

Ademais, o Grupo destaca que embora a aplicabilidade dos contratos e

instrumentos possa ser demonstrada do ponto de vista conceitual, a verificação do efetivo exercício dos direitos dos titulares de dados pessoais no contexto transfronteiriço é uma tarefa mais complexa[25]. Por isso, é necessário avaliar se as entidades participantes das normas corporativas globais são de fato compelidas a cumprir as regras internas[26]. Daí a importância de se investigar se as empresas realizam treinamentos e capacitações voltadas à proteção de dados pessoais, se os colaboradores conhecem as políticas de proteção de dados pessoais e se têm informações sobre o tema facilmente alcançáveis, como, por exemplo, na intranet.

Outrossim, o Grupo ressalta que as normas corporativas globais devem prever a realização de auditorias, bem como o dever de cooperação com as autoridades de proteção de dados pessoais[27]. Por isso, tem-se a obrigação inequívoca de que todas as entidades do grupo corporativo aceitem eventuais auditorias e solicitações realizadas pelas autoridades nacionais[28].

No mais, é imprescindível que todas as partes das normas corporativas globais cumpram as recomendações da autoridade nacional, bem como estabeleçam um sistema de atendimento das reclamações e solicitações dos titulares de dados pessoais[29]. Ainda, é necessário que as normas corporativas globais apresentem disposições sobre a responsabilidade em caso de incidentes envolvendo os dados pessoais[30]. Por fim, é necessário que os grupos corporativos titulares de normas corporativas globais informem aos titulares de dados pessoais sobre a transferência transfronteiriça dos dados[31].

Na prática, a expectativa é que as empresas multinacionais sejam as principais usuárias desses mecanismos, tendo em vista os benefícios oriundos de uma regulamentação uniforme para as transferências intragrupo em todo o mundo. Claro, como os outros mecanismos de salvaguardas trazidos pelas regulações, as normas corporativas globais enfrentam desafios práticos que requerem atenção e soluções eficazes pelas autoridades de proteção de dados. De qualquer sorte, desempenham um papel significativo ao promover a cultura de proteção de dados em escala global, fornecendo um ponto de partida essencial para a transformação de mentalidades nas empresas e, consequentemente, nas pessoas.

4 conclusão

A efetiva regulamentação dos mecanismos de salvaguardas para transferência internacional de dados pessoais no Brasil representa um passo crucial para garantir maior proteção e segurança nessas operações. A atenção dedicada a essa pauta pelas iniciativas da ANPD demonstra o compromisso em alinhar as práticas nacionais aos padrões internacionais.

Considerando as normas corporativas globais, é fundamental reconhecer que, apesar dos desafios práticos inerentes a esses mecanismos, sua importância é incontestável. Além de estabelecerem uma base essencial para a transformação de mentalidades nas empresas, desempenham um papel fundamental na promoção de uma cultura global de proteção de dados.

No âmbito da regulamentação desses mecanismos, a experiência europeia oferece insights valiosos. O Grupo de Trabalho do Artigo 29 apresentou conceitos e práticas essenciais para a eficácia das normas corporativas globais como uma salvaguarda eficaz na transferência internacional de dados pessoais. Isso inclui a incorporação dos princípios legais, aplicação global, vinculação legal e exigibilidade. Além do aspecto teórico, destaca-se que a implementação prática desempenha um papel crucial, exigindo medidas concretas para avaliar a conformidade efetiva, como a realização de treinamentos para os colaboradores, auditorias e cooperação com as autoridades de proteção de dados.

Em última análise, os ensinamentos oriundos da experiência europeia, desempenham um papel crucial para o Brasil. Ao adotar e adaptar essas lições, o Brasil impulsiona o fluxo de trocas econômicas com as empresas aqui estabelecidas, além reforçar sua conformidade com padrões internacionais e aprimorar suas práticas de proteção de dados, contribuindo assim para um ambiente global mais confiável e seguro. Isto é, ao alinhar-se a padrões internacionais, as empresas brasileiras ganham não apenas em termos de conformidade, mas também conquistam a confiança de parceiros comerciais globais.

referências bibliográficas

Binding Corporate Rules. The General Data Protection Regulation. PWC, 2019. Disponível em: https://www.pwc.com/m1/en/publications/documents/pwc-binding-corporate-rules-gdpr.pdf. Acesso em: 23 mar. 2023.

BRASIL. Autoridade Nacional de Proteção de Dados. **Regulamento de Transferências Internacionais de Dados Pessoais e do Modelo de Cláusulas-Padrão Contratuais**. Disponível em: https://www.gov.br/participamaisbrasil/regulamento-de-transferencias-internacionais-de-dados-pessoais-e-do-modelo-de-clausulas-padrao-contratuais. Acesso em: 6 nov. 2023.

BRASIL. Autoridade Nacional de Proteção de Dados. **Tomada de Subsídios sobre Transferência Internacional**. Disponível em: https://www.gov.br/participamaisbrasil/tomada-de-subsidios-transferencia- internacional. Acesso em: 10 mar. 2023.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 out. 2023.

BRASIL. **Portaria nº 11, de 27 de janeiro de 2021**. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-11-de-27-de-janeiro-de-2021-301143313. Acesso em: 24 mar. 2023.

BRASIL. **Projeto de Lei nº 4.060, de 2012** (Apenso PLs nos 5.276/16 e 6.291/16). Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename. Acesso em: 25 fev. 2023.

PRADO CHAVES, Luis Fernado. Da Transferência Internacional de Dados. *In*: MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato. **LGPD: Lei Geral de Proteção de Dados Pessoais Comentada**. 4. Ed. São Paulo: Revista dos Tribunais, 2021, p. RL-1.10. *E-book*. Disponível em: https://proview.thomsonreuters.com/launchapp/title/rt/codigos/188730949/v4/page/RL-1.10. Acesso em: 20 mar. 2023.

PROUST, Olivier; BARTOLI, Emmanuelle. Binding Corporate Rules: a global solution for international data transfers. **International Data Privacy Law**, London, p. 2, November 25, 2011. Disponível em: https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2011/12/International_Data_Privacy_Law-

2011-Proust.pdf. Acesso em: 20 mar. 2023.

REINO UNIDO. Information Commissioner's Office. **Guide to Binding Corporate Rules**. Disponível em: https://ico.org.uk/for-organisations/guide-to-binding-corporate-rules/. Acesso em: 10 mar. 2023.

UNIÃO EUROPEIA. **Artigo 46 - GDPR**. Disponível em: https://gdpr-info.eu/art-46-gdpr/. Acesso em: 06 nov. 2023.

UNIÃO EUROPEIA. European Commission. Article 29 - **Data Protection Working Party**. Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, adopted on 3 June 2003. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf. Acesso em: 20 mar. 2023.

UNIÃO EUROPEIA. **Regulation (EU) 2016/679** of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Chapter 5. Disponível em: https://gdpr-info.eu/chapter-5/. Acesso em: 25 out. 2023.

VERONESE, Alexandre. Transferências internacionais de dados pessoais: o debate transatlântico norte e sua repercussão na América Latina e no Brasil. *In*: BIONI, Bruno. **Tratado de Proteção de Dados Pessoais**. 1. Ed. São Paulo: Grupo GEN, 2020, p. 718. E-book. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 16 mar. 2023.

Notas de rodapé

1 BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 out. 2023.

2 UNIÃO EUROPEIA. **Regulation (EU) 2016/679** of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Chapter 5. Disponível em: https://gdpr-info.eu/chapter-5/. Acesso em: 25 out. 2023.

3 UNIÃO EUROPEIA. **Artigo 46 - GDPR**. Disponível em: https://gdpr-info.eu/art-46-gdpr/. Acesso em: 06 nov. 2023.

4 BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 out. 2023.

5 PRADO CHAVES, Luis Fernado. Da Transferência Internacional de Dados. *In:* MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato. LGPD: **Lei Geral de Proteção de Dados Pessoais Comentada**. 4. Ed. São Paulo: Revista dos Tribunais, 2021, p. RL-1.10. E-book. Disponível em: https://proview.thomsonreuters.com/launchapp/title/rt/codigos/188730949/v4/page/RL-1.10. Acesso em: 20 mar. 2023.

6 BRASIL. **Projeto de Lei nº 4.060, de 2012** (Apenso PLs nos 5.276/16 e 6.291/16). Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename. Acesso em: 25 fev. 2023.

7 BRASIL. **Portaria nº 11, de 27 de janeiro de 2021**. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-11-de-27-de-janeiro-de-2021-301143313. Acesso em: 24 mar. 2023.

8 BRASIL. Autoridade Nacional de Proteção de Dados. **Tomada de Subsídios sobre Transferência Internacional**. Disponível em: https://www.gov.br/participamais-brasil/tomada-de-subsidios-transferencia- internacional. Acesso em: 10 mar. 2023.

9 BRASIL. Autoridade Nacional de Proteção de Dados. **Regulamento de Transferências Internacionais de Dados Pessoais e do Modelo de Cláusulas-Padrão Contratuais**. Disponível em: https://www.gov.br/participamaisbrasil/regulamento-de-transferencias-internacionais-de-dados-pessoais-e-do-modelo-de-clausulas-padrao-contratuais. Acesso em: 6 nov. 2023.

10 BRASIL. Autoridade Nacional de Proteção de Dados. **Regulamento de Transferências Internacionais de Dados Pessoais e do Modelo de Cláusulas-Padrão Contratuais**. Disponível em: https://www.gov.br/participamaisbrasil/regulamento-de-transferencias-internacionais-de-dados-pessoais-e-do-modelo-de-clausulas-padrao-contratuais. Acesso em: 6 nov. 2023.

11 PROUST, Olivier; BARTOLI, Emmanuelle. Binding Corporate Rules: a global solution for international data transfers. **International Data Privacy Law**, London, p.

2, November 25, 2011. Disponível em: https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2011/12/International_Data_Privacy_Law-2011-Proust.pdf. Acesso em: 20 mar. 2023.

12 REINO UNIDO. Information Commissioner's Office. **Guide to Binding Corporate Rules**. Disponível em: https://ico.org.uk/for-organisations/guide-to-binding-corporate-rules/. Acesso em: 10 mar. 2023.

13 **Binding Corporate Rules. The General Data Protection Regulation**. PWC, 2019. Disponível em: https://www.pwc.com/m1/en/publications/documents/pwc-binding-corporate-rules-gdpr.pdf. Acesso em: 23 mar. 2023.

14 **Binding Corporate Rules. The General Data Protection Regulation**. PWC, 2019. Disponível em: https://www.pwc.com/m1/en/publications/documents/pwc-binding-corporate-rules-gdpr.pdf. Acesso em: 23 mar. 2023.

15 VERONESE, Alexandre. Transferências internacionais de dados pessoais: o debate transatlântico norte e sua repercussão na América Latina e no Brasil. *In*: BIONI, Bruno. **Tratado de Proteção de Dados Pessoais**. 1. Ed. São Paulo: Grupo GEN, 2020, p. 718. *E-book*. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 16 mar. 2023.

16 UNIÃO EUROPEIA. European Commission. **Article 29 - Data Protection Working Party**. Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, adopted on 3 June 2003, p. 7. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf. Acesso em: 20 mar. 2023.

17 UNIÃO EUROPEIA. European Commission. **Article 29 - Data Protection Working Party**. Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, adopted on 3 June 2003, p. 7. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf. Acesso em: 20 mar. 2023.

18 UNIÃO EUROPEIA. European Commission. **Article 29 - Data Protection Working Party**. Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, adopted on 3 June 2003, p. 7. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf. Acesso em: 20 mar. 2023.

19 UNIÃO EUROPEIA. European Commission. **Article 29 - Data Protection Working Party**. Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, adopted on 3 June 2003, p. 7. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf. Acesso em: 20 mar. 2023.

20 UNIÃO EUROPEIA. European Commission. Article 29 - Data Protection Working Party. Working Document: Transfers of personal data to third countries: Applying Arti-

cle 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, adopted on 3 June 2003, p. 7. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf. Acesso em: 20 mar. 2023.

21 UNIÃO EUROPEIA. European Commission. **Article 29 - Data Protection Working Party**. Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, adopted on 3 June 2003, p. 7. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf. Acesso em: 20 mar. 2023.

22 UNIÃO EUROPEIA. European Commission. **Article 29 - Data Protection Working Party**. Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, adopted on 3 June 2003, p. 7. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf. Acesso em: 20 mar. 2023.

23 UNIÃO EUROPEIA. European Commission. **Article 29 - Data Protection Working Party**. Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, adopted on 3 June 2003, p. 7. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf. Acesso em: 20 mar. 2023.

24 UNIÃO EUROPEIA. European Commission. **Article 29 - Data Protection Working Party**. Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, adopted on 3 June 2003, p. 7. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf. Acesso em: 20 mar. 2023.

25 UNIÃO EUROPEIA. European Commission. **Article 29 - Data Protection Working Party**. Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, adopted on 3 June 2003, p. 7. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf. Acesso em: 20 mar. 2023.

26 UNIÃO EUROPEIA. European Commission. **Article 29 - Data Protection Working Party**. Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, adopted on 3 June 2003, p. 7. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf. Acesso em: 20 mar. 2023.

27 UNIÃO EUROPEIA. European Commission. **Article 29 - Data Protection Working Party**. Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, adopted on 3 June 2003, p. 7. Disponível em: https://ec.europa.eu/

justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf. Acesso em: 20 mar. 2023.

28 UNIÃO EUROPEIA. European Commission. **Article 29 - Data Protection Working Party**. Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, adopted on 3 June 2003, p. 7. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf. Acesso em: 20 mar. 2023.

29 UNIÃO EUROPEIA. European Commission. **Article 29 - Data Protection Working Party**. Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, adopted on 3 June 2003, p. 7. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf. Acesso em: 20 mar. 2023.

30 UNIÃO EUROPEIA. European Commission. **Article 29 - Data Protection Working Party**. Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, adopted on 3 June 2003, p. 7. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf. Acesso em: 20 mar. 2023.

31 UNIÃO EUROPEIA. European Commission. **Article 29 - Data Protection Working Party**. Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, adopted on 3 June 2003, p. 7. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf. Acesso em: 20 mar. 2023.

SEÇÃO VI

Responsabilidade Civil & Proteção ao Consumidor

Pontos de contato entre a Responsabilidade Civil no Código de Defesa do Consumidor (CDC) e a Lei Geral de Proteção de Dados (LGPD)

Luiza Teotônio

Mauricio Negreira

1 considerações iniciais: relações de consumo e tratamento de dados

A responsabilidade civil no Código de Defesa do Consumidor (CDC) é uma parte importante da legislação brasileira que trata dos direitos e garantias dos consumidores. O CDC estabelece normas que visam proteger os consumidores em suas relações de consumo, garantindo-lhes reparação em caso de danos causados por produtos ou serviços defeituosos ou que apresentam vícios.

O regime de responsabilidade civil adotado pelo CDC determina que as relações de consumo sejam ditadas pela aplicação da responsabilidade civil objetiva[1], ou seja, caberá ao consumidor comprovar que, por meio da relação de consumo existente, este sofreu um dano de esfera moral e/ou material, independentemente da comprovação de culpa por parte do fornecedor.

Importante mencionar que o referido diploma também traz a proteção dos consumidores por equiparação, que são todos aqueles que não tiveram uma relação direta de consumo por meio do produto ou serviço, mas sofreram algum prejuízo ou foram vítimas de determinado evento[2].

Estas regras também são aplicáveis quando o tratamento de dados pessoais for resultante de uma relação de consumo, conforme informado pelo art. 45 da Lei Geral de Proteção de Dados (LGPD) (BRASIL, 2018). Portanto, sempre que o titular dos dados pessoais tiver adquirido um produto ou serviço como destinatário final, este poderá invocar a seu favor o sistema de responsabilização previsto no CDC (MALDONADO *et al*, 2019, p. 331).

Da mesma forma em que os direitos dos consumidores e titulares se conversam, as causas de excludentes de responsabilidade por parte dos fornecedores e dos agentes de tratamento também se equiparam, conforme se observa no quadro comparativo entre as legislações:

CDC	LGPD
Art. 12 [...] § 3° O fabricante, o construtor, o produtor ou importador só não será responsabilizado quando provar: I - que não colocou o produto no mercado; II - que, embora haja colocado o produto no mercado, o defeito inexiste; III - a culpa exclusiva do consumidor ou de terceiro.	Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem: I - que não realizaram o tratamento de dados pessoais que lhes é atribuído; II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.
Art. 14 [...] § 1° O serviço é defeituoso quando não fornece a segurança que o consumidor dele pode esperar, levando-se em consideração as circunstâncias relevantes, entre as quais: I - o modo de seu fornecimento; II - o resultado e os riscos que razoavelmente dele se esperam; III - a época em que foi fornecido.	Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais: I - o modo pelo qual é realizado; II - o resultado e os riscos que razoavelmente dele se esperam; III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

Desta forma, se o tratamento de dados pessoais for resultado de uma relação de consumo, as partes deverão observar seus respectivos direitos e deveres abarcados tanto na LGPD, quanto no CDC.

2 da excludente de responsabilidade por caso fortuito e da força maior aplicado ao CDC com reflexos na LGPD

É forte a corrente doutrinária de que o rol de excludentes no CDC é taxativo, não se admitindo outros fatores obstativos de nexo de causalidade ou da ilicitude. Todavia, há outra visão de que os eventos imprevisíveis e inevitáveis podem ser considerados excludentes da responsabilidade[3].

Neste sentido, adentramos ao conceito dos institutos do caso fortuito e da força maior, sendo que, em uma breve explicação, podemos classificar o primeiro como um evento totalmente imprevisível, enquanto o segundo, é um evento previsível, mas inevitável (GOMES, 1997, p. 148).

Frente a este cenário, o caso fortuito e a força maior podem ser enquadrados como causas de exclusão de responsabilidade civil do fornecedor, embora não previstas expressamente no CDC. O fundamental é que o acontecimento inevitável ocorra fora da esfera de vigilância do fornecedor, geralmente, após a colocação do produto no mercado, tendo força suficiente para romper a relação de causalidade (SANSEVERINO, 2010, p. 312).

Entretanto, este entendimento apresenta limitações, visto que, conforme determinado pelo Enunciado nº 443 da V Jornada de Direito Civil (CJF, 2012), o caso fortuito e a força maior somente serão considerados como excludentes de responsabilidade civil quando o fato gerador do dano não for conexo à atividade desenvolvida.

Desse modo, é preciso relacionar o evento com a atividade desenvolvida pelo agente, ou seja, com o risco do empreendimento, risco do negócio ou risco-proveito[4], remontando à divisão destes eventos em internos e externos (TARTUCE, 2023, p. 303). Um evento interno possui relação com o negócio desenvolvido, não excluindo a responsabilidade civil, já o evento externo é totalmente estranho ou alheio ao negócio, excluindo o dever de indenizar (TARTUCE, 2023, p. 617).

Podemos encontrar exemplos destes eventos em julgados de nossos tribunais, como quando ocorre um assalto a mão armada a ônibus, concluindo o tribunal tratar-se de fortuito externo, pois não é essencial ao negócio a segurança do passageiro de modo a impedir o evento[5].

Por outro lado, entende-se que o assalto a um banco não constitui um evento externo, pois ingressa no risco do negócio, não afastando o dever de reparar da instituição respectiva, o que está em plena sintonia com a ideia de risco-proveito do Código do Consumidor[6].

3 considerações finais: o encontro entre LGPD e CDC

Partindo para uma análise comparativa com o tratamento de dados pessoais, um ataque hacker que inviabilize a funcionalidade de sistemas e/ou divulgue indevidamente dados pessoais de titulares pode ser enquadrado como caso fortuito e força maior ou estará alocado como um risco-proveito do negócio?

Para se chegar a esta resposta, é importante avaliar qual a finalidade do negócio executado pelo agente de tratamento que sofreu o ataque, visto que, caso a finalidade da atividade envolva a utilização de dados e/ou tecnologias, a garantia de segurança das informações presentes na atividade é um risco do negócio, podendo ser enquadrada como um fortuito interno, e por consequência, o dever de indenizar os prejuízos aos titulares poderá existir[7].

Evidente que o estado atual da técnica sempre impactará nos riscos relacionados à atividade de tratamento de dados pessoais, e na segurança ao redor dessas atividades, e é muito salutar que o legislador pondere esse fato entre as circunstâncias que levem à determinação da presença ou ausência de segurança que o titular dos dados pode esperar, o que representa impacto direto na responsabilização (MALDONADO *et al*., 2019, p. 330).

Nenhum sistema é a prova de falhas ou vulnerabilidades, até porque a tecnologia evolui na mesma proporção (ou até mais rápido) que a tecnologia para defesa desses incidentes. Por conta disso, nunca se pode esperar uma absoluta segurança em sistemas tecnológicos.

Sendo assim, um caminho a se seguir seria a adoção de melhores técnicas pelo controlador e operador para protegerem seu ambiente, caso a invasão resulte de técnicas inovadoras. Assim, comprovada a adoção de medidas de segurança eficientes e razoáveis, admite-se a excludente de responsabilidade por fato de terceiro, que pode exonerar integralmente a responsabilidade ou mitigá-la (MALDONADO *et al*., 2019, p. 329).

Na mesma linha, entende Bioni e Dias (2020, p. 16) ao afirmarem que "os agentes devem [...] ajustar suas medidas de segurança para corresponder à probabilidade e à gravidade que violações podem assumir em faze do impacto a direitos e liberdades dos titulares". Desse modo, aponta os autores, deve se considerar um espécie de "gradiente ou filtro catalisador da culpa", correlacionando-o com a responsabilidade civil dos agentes.

Assim, ainda que o debate sobre responsabilidade civil subjetiva ou objetiva dos agentes tenha seu valor, considera-se que o caminho para um ambiente seguro aos consumidores e, concomitantemente, titulares de dados, seria a cha-

mada accountabiliy. Por isso, quanto maior for o risco relacionado à atividade de tratamento destes agentes, maiores esforços deverão ser empreendidos para a segurança dos dados tratados.

referências bibliográficas

BRASIL. **Código de Defesa do Consumidor**. Lei nº 8.078, de 11 de setembro de 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 15 out. 2023.

_____. **Lei Geral de Proteção de Dados Pessoais**. Lei n. 13.709, de 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.html. Acesso em: 15 out. 2023.

BIONI, Bruno; DIAS, Daniel. **Responsabilidade civil na proteção de dados pessoais**: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. Civilistica.com. Rio de Janeiro, a. 9, n. 3, 2020. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/662/506. Acesso em: 20 jun. 2023.

CJF, Conselho de Justiça Federal. **V Jornada de Direito Civil**. 2012. Disponível em: https://www.cjf.jus.br/enunciados/enunciado/356. Acesso em: Acesso em: 15 out. 2023.

MALDONADO, Nóbrega *et al*. **Lei Geral de Proteção de Dados Comentada**. 2ª Edição. 2019. Editora: Revista dos Tribunais.

GOMES, Orlando. **Obrigações**. 11 ed. Atualizada por Humberto Theodoro Júnior. Rio de Janeiro. Forense, 1997.

SANSEVERINO, Paulo de Tarso Vieira. **Responsabilidade Civil no Código do Consumidor e a defesa do Fornecedor**, 2ª ed. Editora: Saraiva, 2010.

TARTUCE Flávio. **Responsabilidade Civil**. 5ª Edição. 2023. Editora: Forense.

notas de rodapé

1 Arts. 12 e 14 da Lei 8.078/90.

2 Art. 17 da Lei 8.078/90: Para os efeitos desta Seção, equiparam-se aos consumidores todas as vítimas do evento.

3 Art. 393 do Código Civil: O devedor não responde pelos prejuízos resultantes de caso fortuito ou força maior, se expressamente não se houver por eles responsabilizado.

4 Segundo a Teoria do Risco-Proveito, todo aquele que fornece produto ou serviço no mercado de consumo auferindo lucro (proveito) responde por eventuais danos, independentemente da comprovação de dolo ou culpa (risco da atividade). O conceito é disseminado pelo TJDF. Disponível em: https://www.tjdft.jus.br/consultas/jurisprudencia/jurisprudencia-em-temas/cdc-na-visao-do-tjdft-1/principios-do-cdc/teoria-do-risco-proveito-da-atividade. Acesso em: 19 out. 2023.

5 Conforme STJ: REsp 726.371/RJ, 4ª Turma, Rel. Min. Hélio Quaglia Barbosa, j. 07.12.2006, DJU 05.02.2007, p. 244.

6 Assim, com variações na argumentação desenvolvida, encontramos também em: STJ, REsp 1093617/PE, 4ª Turma, Rel. Min João Otavio de Noronha, j. 17.03.2009, DJE 23.03.2009; STJ, REsp 787.124/RS, 1ª Turma, Rel. Min José Delgado, j. 20.04.2006, DJ 22.05.2006, p. 167; STJ, REsp 694.153/PE, 4ª Turma, Rel. Min. Cesar Asfor Rocha, j. 28.06.2005, DJ 05.09.2005, p. 429; STJ, REsp 613.036/RJ, 3ª Turma, Rel. Min. Castro Filho, j. 14.06.2004, DJ 1.º.07.2004, p. 194. Vide TARTUCE Flávio. Responsabilidade Civil. 5ª Edição. 2023. Editora: Forense. p. 618.

7 Sobre esse tema, recomendamos também: Proc. nº 0026768-65.2021.8.16.0014. Des. Angela Khury, 10ª Camara Cível TJ-PR. Julgado em 20/04/2022 e TJSP; Apelação Cível 1057402-47.2022.8.26.0100; Relator (a): Issa Ahmed; Órgão Julgador: 34ª Câmara de Direito Privado; Foro Central Cível - 28ª Vara Cível; Data do Julgamento: 27/06/2023; Data de Registro: 27/06/2023.

SEÇÃO VII

Regulação de novas tecnologias

Algorithmic Impact Assessment (AIA) e regulação de Inteligência Artificial

Luis Acioly

1 introdução

No horizonte da regulação de tecnologias, uma gama de desafios é posta ao processo normativo, especialmente quanto aos prismas de eficiência e legitimidade. Além do problema de ritmo, isto é, o acompanhamento do Estado do desenvolvimento de novas tecnologias, há obstáculos relacionados ao grau de intervenção em determinada fase do desenvolvimento dessa tecnologia e à desconexão regulatória, quando o surgimento dessa tecnologia se torna obsoleta as normas regulatórias e setoriais pré-existentes (MOSES, 2014).

Nesse contexto, regulações fechadas, pautadas em uma lógica de comando e controle tem sua eficácia questionada, ao tempo que surgem novas formas de relacionamento entre o Estado e os agentes econômicos na dinâmica regulatória (BALDWIN; CAVE, 1999). Abordagens de um mandato regulatório cooperativo tem surgido como forma de dotar o agente econômico de certa discricionaridade, mediante divisão de tarefas e designação de elementos de prestação de contas (BIONI, 2022).

Essa dinâmica regulatória se materializa através de mecanismos de prestação de contas, a partir dos quais é possível apontar um comportamento necessário ao agente regulador, seja na formulação das políticas regulatórias, seja no *enforcement* em um esquema reação equivalente, em um panorama de regulação responsiva (ARANHA, 2023).

2 avaliação de impacto algorítmico e sua primazia regulatória

No ecossistema da regulação de inteligência artificial, a cognição de riscos é um elemento estruturante das políticas regulatórias, notadamente a partir de avaliações de impacto. Ademais, os impactos do uso de sistemas de IA em grupos historicamente vulnerabilizados tem demonstrado a necessidade de acompanhamento e estratificação dos riscos decorrentes do implemento crescente dessa tecnologia no cotidiano social (NEGRI *et al*., 2023).

Estruturas regulatórias em diversos sistemas normativos têm apontado instrumentos de prestação de conta no contexto do desenvolvimento e aplicação de sistemas de IA, dentre as quais se pode citar o Reino Unido e a Espanha, a partir da regulamentação específica da proteção de dados pessoais em tratamento automatizado de dados pessoais (LEMOS *et al*., 2023), o Canadá, a partir da proposta normativa que consubstancia o "*Artificial Intelligence and Data Act*" ou, e a União Europeia, no contexto da proposta do "*Artificial Intelligence Act*", que busca vincular seus Estados-membros.

A adoção de mecanismos de avaliação de impacto tem norteado sistemas regulatórios em diversas áreas, maiormente como pressuposto à concessão de permissão administrativa para pesquisa ou execução de projetos comerciais ou públicos (RAAB, 2020). Uma avaliação de impacto é um processo específico para avaliar e documentar os impactos de um dado projeto ou empreendimento em determinadas áreas ou a partir de determinadas abordagens, e atribuir responsabilidades na mitigação desses impactos (RAAB, 2020).

Nesse cenário, a Avaliação de Impacto Algorítmico ("*Algorithmic Impact Assessment*" ou "*AIA*") se desponta por sua função eminentemente relacional, como instrumento de prestação de contas e cognição e gestão de riscos envolvendo uso de IA. A AIA é considerada um instrumento mais amplo do que a Avaliação de Impacto à Proteção de Dados, na medida em que não se esgota nos aspectos inerentes aos dados pessoais, mas relaciona-se com a própria programação algorítmica e com o aprendizado de máquina (LEMOS *et al*, 2023).

Watkins *et al* (2021) asseveram que o termo "*Algorithmic Impact Assessment*" tem sido utilizado em uma diversidade de circunstâncias, direcionando de forma genérica um processo de avaliação e documentação da verificação dos possíveis impactos a direitos e seus consequentes danos na alçada de um sistema de inteligência artificial.

Reisman *et al* (2018) sustentam quatro objetivos políticos na inclusão da Avaliação de Impacto Algorítmico nas estruturas regulatórias, a partir de uma

agenda pública em IA: (i) respeitar o direito de o público conhecer quais sistemas impactam em suas vidas, a partir da descrição pública dos sistemas de decisão automatizada que afetam significativamente indivíduos e coletividades; (ii) aumentar a expertise dos órgãos públicos na capacidade de avaliar sistemas construídos ou adquiridos pela administração pública, antecipando questões com potencial de gerar preocupações sociais; (iii) garantir uma maior responsabilidade dos sistemas de decisão automatizada, fornecendo uma oportunidade de auditores externos identificarem possíveis problemas e pontos de aprimoramento; e (iv) garantir que o público tenha a oportunidade significativa de responder e contestar o uso de um determinado sistema ou abordagem algorítmica para a autoridade competente.

No panorama do Projeto de Lei n. 2.338, de 2023, a Avaliação de Impacto Algorítmico é disposta em seus art. 24, que prevê a obrigatoriedade de ela, ao menos, registrar: (i) os riscos conhecidos e previsíveis à época da elaboração do sistema inteligente; (ii) os benefícios associados ao sistema; (iii) a probabilidade de efeitos adversos e a quantidade de pessoas possivelmente impactadas; (iv) a gravidade das consequências e as medidas de mitigação; (v) a lógica do funcionamento do sistema inteligente; (vi) o processo e resultado dos testes e avaliações para verificação de possíveis impactos a direitos; (vii) o treinamento e ações de conscientização dos riscos associados ao sistema; (viii) as medidas de mitigação e justificação do risco residual; e (ix) as medidas de transparência pública, especialmente quanto aos possíveis usuários desse sistema.

Contudo, o artigo 24 do PL, na forma como fora protocolado junto ao Congresso Nacional, não apresenta a necessidade de elaboração prévia da AIA, como o faz em relação à análise preliminar, tal como apontado na doutrina de Selbst (2021) e Reisman *et al* (2018). De forma semelhante, a minuta da propositura legislativa não contempla mecanismos de notificação e comentários públicos, nem outra forma de participação dos possíveis afetados no processo de avaliação, sendo previsto somente a necessidade de publicização do seu resultado.

3 **considerações finais**

Importa consignar que a Avaliação de Impacto Algorítmico desponta como instrumento de prestação de contas e alocação de responsabilidades, no contexto da regulação da IA a partir de uma estrutura de cognição, gestão e avaliação de consequências do uso de inteligência artificial, para fins de ponderação de

um comportamento regulatório responsivo, coerente com carga de risco demonstrada na avaliação. Deve-se caminhar, ainda, para o aprimoramento da estrutura desse instrumento de *accountability*, no processo legislativo brasileiro, a partir da inserção de mecanismos de participação popular na condução do processo avaliativo e viabilização do fórum público de prestação de contas.

referências bibliográficas

ARANHA, M.I. **Manual de Direito Regulatório**: Fundamentos de Direito Regulatório. 8. ed. rev. ampl. London: Laccademia Publishing, 2023.

BALDWIN, R.; CAVE, M. **Understanding Regulation**: Theory, Strategy, and Practice. Oxford: Oxford University Press, 1999.

BIONI, B.R.. **Regulação e Proteção de Dados Pessoais**: O Princípio da Accountability. Rio de Janeiro: Forense, 2022.

LEMOS, A.; BUARQUE, G.; SOARES, I.; MULIN, V.; CHIAVONE, T.. **Avaliação de Impacto Algorítmico para a proteção dos direitos fundamentais**: Relatório. Brasília: Laboratório de Políticas Públicas e Internet, 2023.

MOSES, L.B. **How to Think About Law, Regulation and Technology**: Problems with 'Technology' as a Regulatory Target. *In:* Innovation and Technology, 1-20(2013). (2013) 5(1); UNSW Law Research Paper No. 2014-30. Disponível em: <http://ssrn.com/abstract=2464750>. Acesso em: 11 jun. 2023.

NEGRI, S. M. C. de Á.; MACHADO, J. de S.; GIOVANINI, C. F. R.; BATISTA, N. P. R.. **Sistemas de Inteligência Artificial e Avaliações de Impacto para Direitos Humanos**. *In:* Revista Culturas Jurídicas, v. 10, Ahead of Print, 2023, p. 1-26. Disponível em: <https://periodicos.uff.br/culturasjuridicas/article/view/56809>. Acesso em: 09 set. 2023.

RAAB, C. **Information privacy, impact assessment, and the place of ethics**. *In:* Computer Law & Security Review, v. 37, jul. 2020, p. 1-16. Disponível em: <https://doi.org/10.1016/j.clsr.2020.105404>. Acesso em: 17 set. 2023.

REISMAN, D.; SCHULTZ, J.; CRAWFORD, K.; WHITTAKER, M.. **Algorithmic Impact Assessment**: a practical framework for public agency accountability. AI NOW, 2018.

SELBST, A. **An institutional view of algorithmic impact assessment**. *In:* Havard Jornal of Law & Technology, Massachusetts, v. 35, n. 1, p. 117-173, 2021. Disponível em: <https://jolt.law.harvard.edu/assets/articlePDFs/v35/Selbst-An-Institutional-View-of-Algorithmic-Impact-Assessments.pdf>. Acesso em: 05 mar. 2023.

WATKINS, E. A.; MOSS, E. METCALF, J.; SINGH, R.; ELISH, M. C. **Governing algorithmic systems with impact assessments**: six observations. *In:* Procee-

dings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society, Nova York, mai., 19-21, p. 1010-1021, 2021, Virtual Event. Disponível em: <https://dl.acm.org/doi/10.1145/3461702.3462580>. Acesso em: 05 mar. 2023.

Accountability, da Teoria Prática: casos de (in)sucesso prestando contas e gerenciando risco jurídico-regulatório

Cristyane Bastos

1 objetivo e abordagem

Este capítulo visa abordar aspectos de relevância, sob uma ótica prática, a respeito dos benefícios e consequência de atender as diretrizes norteadoras do princípio da accountability no que tange a proteção de dados pessoais, considerando, para tanto, a realidade das organizações brasileira, e quanto este princípio se tornar facilitador da atividade regulatória do órgão competente, qual seja, a Agência Nacional de Proteção de Dados Pessoais - ANPD.

Ademais, tal princípio coloca no centro o principal ator beneficiado pela Lei nº 13.709 de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais – o titular de dados pessoais – o qual, pelo fundamento da autodeterminação informativa[1], se torna aquele ao qual se deve prestar contas a respeito da finalidade e cautelas que uma organização vem tomando no tratamento dos dados pessoais.

Considerando, agora, a perspectiva dos agentes de tratamento, o princípio da accountability se torna verdadeira ferramenta auxiliar da criação de cultura, responsabilidade, e compromisso na proteção dos dados pessoais aos quais tem acesso em decorrência das atividades exercidas. Deve ser uma constante preocupação

do controlador ou operador manter os registros de suas atividades e atestar efetivamente que está em conformidade com os ditames da Lei Geral de Proteção de Dados Pessoais - LGPD e demais legislações que compõe o microssistema normativo regente da matéria.

2 **conceito e contextualização**

O princípio do accountability resulta de avanços e evoluções conceituais e entendimentos durante várias etapas do amadurecimento sobre o tema nos países e organizações precursoras sobre o tema. Assim também ocorreu no Brasil, durante os debates legislativos para edição da Lei Geral de Proteção de Dados Pessoais.

Resultado desta evolução, o art. 6º, X, da LGPD, determina que as atividades de tratamento de dados pessoais deverão observar a boa-fé e dentre outros princípios aquele que prevê a necessária "demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas".

Nesse sentido, ao debater o tema sob a perspectiva conceitual, Bruno Bioni, em sua obra[2], esclarece que a função do princípio "é muito mais do que ser simplesmente transparente, já que a tão desejada virtuosidade deriva necessariamente do reconhecimento de outrem e não apenas de dar publicação acerca de suas ações".

Assim, é possível identificar os atores responsáveis por essa missão, aqueles os quais devem prestar contas e responsabilidades de maneira fidedigna no que se refere ao tratamento de dados pessoais, e de outro lado aqueles aos quais as contas necessitam ser prestadas.

Os agentes de tratamento de dados pessoais - controladores e operadores - são responsáveis por demonstrar a conformidade da organização no que tange ao atendimento dos direitos dos titulares. Além disso, cabe esses agentes responder quando inquiridos pela Agência Nacional de Proteção de Dados - ANPD, e demais órgãos que envolvem o microssistema relacionado à matéria. Nesta seara, inclui-se órgãos como o PROCON e os órgão judicantes.

Porém, é importante lembrar que estes mesmos órgãos também podem estar na posição de responsáveis e prestadores de contas em relação ao tratamento de dados pessoais realizados na organização. Então, caso estejam na posição de controladores ou operadores, se posicionarão como aqueles que devem prestar as informações, já que lei nacional consolidada de proteção de dados, prevê como agentes de tratamento toda pessoa jurídica de direito público ou privado que realize trata-

mento de dados pessoais em suas atividades.

Ainda, a própria Agência Nacional de Proteção de Dados - ANPD, tem o dever de prestar contas perante a sociedade em relação as suas atividades, por meio de apresentação de relatórios anuais, incluindo aqueles financeiros e planos de ação, apresentar o resultado das consultas públicas relacionadas as normativas que são produzidas pelo órgão, disponibilizar a avaliações de risco regulatórios, e trazer documentos de apoio para melhor elucidar os pontos da Lei.

A legislação nacional permite aos agentes de tratamento uma certa discricionariedade no que diz respeito a atestação da conformidade com os ditames da norma, mas não abre mão de que o titular reconheça os esforços da organização, de maneira efetiva, de modo que seja também facilmente observada por qualquer órgão que fiscalize ou avalie o cumprimento da normativa, ainda que em âmbito judicial.

Porém, em que pese essa discricionariedade, o fato é que a própria legislação trouxe indícios que podem culminar na atestação e demonstração de responsabilidade do agente de tratamento. Nesse intuito, é possível afirmar que se a organização implementar os ditames do art. 50 da Lei, que trata de boas práticas e governança em proteção de dados pessoais, estará seguindo um verdadeiro guia, que se praticado de forma que se coaduna com a realidade do agente, trará fortes atestações, associados aos documentos de registro trazidos, também, na própria legislação.

O fato é que, de uma maneira simplista, o princípio estudado perpassa não apenas pela busca da comprovação, mas seja efetivo em demonstrar como ocorre o fluxo de dados dentro da organização – se estão sendo atribuídas corretas bases legais e finalidades para o tratamento de dados pessoais, se há tratamento de dados pessoais de grande impacto aos direitos do titular, com quem há compartilhamento desses dados, como se dá e em que prazo descarta-os, e como a organização cuida e quais salvaguardas e contramedidas estão estruturadas para minimizar os riscos à confidencialidade, integridade e disponibilidade desses dados[3].

Ademais, essa comunicação, seja quem for a parte interessada, deverá ser intuitiva, de linguagem simples, e de fácil compreensão, mesmo que se tratem de registros regulatórios. O importante é que toda comprovação traga consigo a realidade do tratamento de dados pessoais acessíveis a qualquer um que as requisita-las.

Nesse ponto, cabe ainda trazer uma necessária preocupação com as pessoas portadoras de deficiência. O agente de tratamento deve trazer acessibilidade a esses registros, de modo que qualquer parte interessada possa se valer dos meios disponibilizados pelo agente para acessar as informações pleiteadas.

O próprio canal de atendimento ao titular de dados pessoais, indispensável ferramenta que dá acesso ao efetivo *accountability*, deve considerar a acessibilidade de

todos, de maneira indiscriminada para que essa prestação de contas seja, de fato, universal.

3 *accountability* na prática: documentos e registros dos agentes de tratamento

Existe grande número de possibilidades no que diz respeito a atestação do cumprimento das diretrizes da legislação e atendimento aos direitos dos titulares. Porém, há registros e documentos que são indispensáveis e que retratam a realidade das operações, riscos e medidas adotadas pelo agente de tratamento. Tais documentos, inclusive, podem ser exigidos pela ANPD, conforme determina a legislação[4].

Assim, é válido, desde já, fazer referência aos chamados documentos entregáveis - aqueles os quais minimamente devem ser produzidos pelo agente de tratamento em caso de eventual questionamento. Dentre eles estão os documentos previstos na própria Lei.

Iniciando por aquele que representa o registro das operações de tratamento de dados pessoais, com as suas respectivas informações que devem considerar, no mínimo, as finalidades de tratamento, os responsáveis, bases legais que fundamentam o tratamento, os titulares de dados envolvidos, com quem os dados são compartilhados – inclusive se há transferência internacional – prazo de descarte e se há tratamento de dados sensíveis e de crianças e adolescentes.

Importante lembrar que os agentes de tratamento de pequeno porte, considerados como tal pela Resolução nº 2 de 2022 da ANPD, poderão apresentar modelos simplificados do referido documento, cujo template já está disponível no sítio eletrônico do órgão regulador.

Outro registro que poderá ser exigido pela ANPD, é aquele relacionado aos impactos de uma atividade que possa trazer riscos consideráveis aos direitos do titular, aí incluídos os previstos na lei e aqueles que de pronto é possível identificar tal necessidade. Como exemplo, temos os seguintes: aqueles que tenham por base legal o legítimo interesse; quando há tratamento de dados sensíveis; tratamentos de dados pessoais em grande volume; tratamento de dados de crianças e adolescentes; quando há transferências internacionais de dados pessoais, dentre outros.

Além destes, a elaboração de políticas, manuais, procedimentos operacionais padrões, avisos de privacidade, devidamente divulgados, preferencialmente no site e na intranet da empresa, de maneira clara e transparente, são fortes atestações de que a organização está objetivando prestar contas aos titulares de dados pessoais,

e está apta a demonstrar suas atividades perante os órgãos que a venham inquirir.

Não é redundante lembrar que uma Política de Privacidade e Proteção de Dados Pessoais deve refletir a realidade da organização em relação as suas operações que envolvam tratamento de dados pessoais. Além de respeitar as exigências previstas no art. 9º da Lei, deve se coadunar com o que foi mapeado e relacionado no inventário de dados pessoais, trazendo uma leitura simples e de fácil acesso a todos.

Nesse mesmo sentido, os avisos de privacidade devem ser claros e abordar os tratamentos de dados pessoais realizados, as finalidades, os direitos daquele titular, os compartilhamentos realizados e o prazo de descarte.

Políticas internas e manuais devem ser claros, disponíveis e de fácil acesso, privilegiando uma comunicação assertiva a acessível a todos os públicos da organização, inclusive as pessoas portadoras de deficiência, com efetiva comunicação e treinamento das partes interessadas, atestado tais treinamentos e reciclagens com listas de frequência e mesmo com realização de gamificação e entrega de certificados.

Aqui ainda é importante ressaltar a necessária demonstração que o agente de tratamento possui políticas e manuais referentes à comunicação de incidentes em segurança da informação às partes interessadas, planos de ação e recuperação de desastre e ainda um plano de continuidade de negócios. Nesse ponto, é importante que a organização, em caso de algum incidente, registre todas as ações realizadas, isole o local, seja em ambiente físico ou virtual, para realização de análises e perícias, a forma e prazo de comunicação aos titulares de dados pessoais e a ANPD, e, se houve necessidade, de acionamento do plano de continuidade de negócios.

Concluindo as observações sobre as políticas e manuais, insta ainda demonstrar que tais documentos devem ser constantemente revisados e atualizados, já que as organizações não são estanques, e continuamente introduzem novos processos de negócio, novos colaboradores e novas contratações. Portanto, atestar o versionamento, a publicização, comunicação e treinamento das versões, é indispensável para o *accountabillity* da organização[5].

Quanto ao consentimento, esta base legal exige que a concessão pelo titular seja feita de maneira expressa e represente a vontade livre deste, nos termos do art. 8º da lei. E, nesse mesmo sentido, no parágrafo segundo do referido artigo, há determinação expressa no sentido que "cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei". Assim, torna-se indispensável que o agente de tratamento registre por documentação física ou outro meio eficiente que de que houve o consentimento do titular, informando-o do direito de revogá-lo a qualquer momento. Esse tipo de atestação é importante para

fundamentar o uso correto da base legal, quando a organização for eventualmente instada a comprovar o regular tratamento dos dados pessoais.

Ademais, é importante ressaltar que a organização deve manter em seus registros, quando do atendimento aos demais pedidos dos titulares de dados pessoais, relacionados aos direitos previstos na Lei, a comprovação da condução e resposta às demandas. Nesse ponto, pode ser recomendado o uso de sistemas encontrados no mercados que facilitam não somente o atendimento com fornecimento de números de protocolo, como apresentando a situação do pedido na organização e a conclusão deste. Estes sistemas podem ainda gerar relatórios de atendimento, como um grande auxiliar na comprovação do atendimento aos pleitos do titular.

Porém, caso se torne oneroso tal medida para a organização, nada impede que sejam registrados e-mails de tratamento das demandas, ou degravações de atendimentos com protocolos no canal telefônico, registros físicos facilitados, dentre outros. É indispensável o registro como comprovação deste atendimento, não importa a forma, contanto que atenda ao titular, e que seja de forma acessível e no tempo previsto na legislação.

4 **considerações finais**

Por fim, retomando tudo que acima foi dito, destaca-se que os documentos e registros acima referidos não findam em si mesmo, há sempre outras possibilidades de ser atestado que o agente de tratamento se preocupa de fato com o que ocorre na organização em termos de proteção de dados pessoais dos *stakeholders*.

referências bibliográficas

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Promulgada em 14 de agosto de 2018. Diário Oficial da União, Brasília, DF, 15 ago. de 2018. Disponível em: [https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm]. Acesso em: (04 de outubro de 2023).

BIONI, Bruno Ricardo. **Regulação e proteção de dados pessoais**: o princípio da accountability. Bruno Ricardo Bioni. – 1. ed. – Rio de Janeiro: Forense, 2022.

DONEDA, Danilo; MENDES. Laura Schertel.; RODRIGUES JR. Otavio Luiz.; BIONI, Bruno Ricardo. **Tratado de proteção de dados pessoais**/Adriana Espindola Corrêa... [*et al.*]; coordenação Danilo Doneda... [*et al.*]. 2ª ed. – Rio de Janeiro: Forense, 2023.

MALDONADO, Viviane Nóbrega. LGPD: **Lei Geral de Proteção de Dados Pessoais**: Manual de Implementação/coordenação Viviane Nóbrega Maldonado. – 2. ed. rev., atual. e ampl – São Paulo: Thomson Reuters Brasil, 2021.

MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato. **LGPD: Lei Geral de Proteção de Dados Pessoais comentada**/ coordenadores Viviane Nóbrega Maldonado e Renato Opice Blum. – 3. ed. rev., atual. e ampl. - - São Paulo: Thomson Reuters Brasil, 2021.

notas de rodapé

1 Nesse sentido, Opice Blum e Ana Maria Roncaglia (2021), ao conceituar a autodeterminação informativa, fazem no seguinte sentido: "É a chamada autodeterminação informativa, que a LGPD trouxe como um dos seus fundamentos, inspirada no conhecido precedente do censo alemão de 1983, que definiu como o poder conferido ao indivíduo de decidir se e em qual extensão serão expostos aspectos da sua vida pessoal".

2 BIONI, Bruno Ricardo. Regulação e proteção de dados pessoais: o princípio da accountability/ Bruno Ricardo Bioni. – 1. ed. – Rio de Janeiro: Forense, 2022. p. 76.

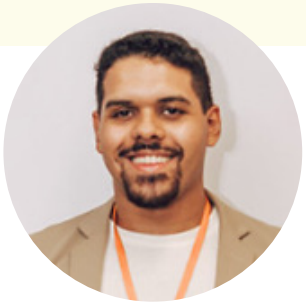
3 É o que aborda, neste mesmo sentido, Walter Aranha Capanema (2021), afirmando que "Os registros, em especial, são ferramentas importantes na medida em que fazem prova positiva da existência de um programa, demonstrando a efetiva preocupação da entidade com o tema e a concretude das medidas adotadas."

4 Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial. Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

5 Assim leciona Fabiano Menke e Guilherme Damasio Goulart (2023) "Não basta a criação desses documentos. Eles precisam ser constantemente revistos e reanalisados, verificando-se se os dados pessoais estão sendo devidamente protegidos e resguardados de riscos internos e externos. Até porque, a atividade de verificação de conformidade (*compliance*) é um processo contínuo"

Conclusão



Pedro Henrique Santos

Analista acadêmico na Associação Data Privacy Brasil de Pesquisa e co-produtor do podcast Dadocracia. Mestrando em direito pela UFMG (Universidade Federal de Minas Gerais) e Graduado em direito pela UFJF (Universidade Federal de Juiz de Fora).

Chegamos ao fim desse verdadeiro mosaico da proteção de dados. Em 7 seções riquíssimas, esperamos que você tenha gostado da leitura e que retorne outras vezes. Os temas abordados envolveram cultura, design e privacidade; a importância de se pensar a proteção de dados na saúde, escolas, infância e adolescência; segurança da informação; a intersecção entre LGPD e demais diplomas legais e um pouco do que poderá ser a regulação da inteligência artificial.

Esse é um espaço de compartilhamento muito especial da comunidade Data Privacy Brasil e representa o que há de melhor na construção de uma cultura de proteção de dados e que pensa nos impactos de novas tecnologias.

Mais do que um horizonte normativo, buscamos oferecer novas formas de pensar que são resultado de grandes discussões levadas a cabo por nossa comunidade. A ciência é um procedimento social complexo, ou seja, depende de pessoas para poder existir, se reproduzir e aprimorar. O Entrelinhas é uma prova do que esse processo pode realizar a partir de nossa comunidade cativa e dedicada, capaz de revelar um futuro de novas possibilidades e de convivência com as novas tecnologias.

Falando em futuro, é sobre isso que este trabalho quer dizer. Em cada capítulo, temos perspectivas distintas sobre os problemas, diagnósticos e soluções para os desafios do presente no que tange ao fluxo de dados em nossa sociedade e das tecnologias contemporâneas. Não é uma tarefa fácil dada a velocidade com que as tecnologias da informação mudam e nos

afetam. É como pintar um quadro sem tela e mesmo assim conseguir expressar o que se deseja.

Nessa tarefa árdua, deixamos nossos agradecimentos especiais para Daiane Conde, Julie Borges, Bárbara Kunde Steffens, Luciano Escobar, Vanessa Santos, Juliana Brasileiro, Franklin Jeferson, Pollyana Moreira, Carmen Arriagada, Thúlio Silveira, Fernando Vasconcelos, Bruna Cruz, Fernanda Ratzkowski, Luiza Teotônio, Mauricio Negreira, Ricardo Maffeis, Ana Carolina Teles, Luis Acioly e Cristyane Bastos. Nas 7 seções deste trabalho, foi com vocês que o nosso leitor passeou.

E acredito que tenha sido ótimo.

Até a próxima!

Agradecimentos

Pedro Martins

Bacharel e Mestre em Direito pela Universidade Federal de Minas Gerais. Desenvolve pesquisa na área de proteção de dados pessoais e profiling. Pesquisador do grupo de pesquisa Persona e Coordenador Acadêmico do Data Privacy Brasil.

É com grande satisfação que expressamos nossa gratidão a todos os colaboradores que tornaram possível a realização deste e-book. Esta obra é fruto de um esforço coletivo e comunitário, concretizando não só no conteúdo, mas também na forma e no modo de fazer a missão da Data Privacy Brasil na promoção de direitos digitais e da proteção de dados por meio da coletividade.

Ao longo do processo de elaboração do conhecimento que está materializado nesse e-book, vivenciamos momentos marcantes com as quatro edições do *Data Talks*, um espaço muito rico e único em que profissionais com backgrounds e experiências muito distintas se reuniram para apresentar sua visão sobre algum tema de fronteira da regulação da proteção de dados no Brasil. Essa troca de experiências por si só já é muito rica, sendo a materialização dessa troca em forma de um livro um verdadeiro gesto de generosidade de todos autores que tomaram seu tempo para refletir, elaborar e compartilhar aquilo que aprenderam. Não poderia haver momento melhor para lançar um livro dessa natureza do que durante as comemorações do Dia da Privacidade em 2024.

Um agradecimento especial ao Gedeão França, Community Manager da Data Privacy Brasil, cujo trabalho incansável foi fundamental para a realização do projeto do Data Talks e a organização deste e-book. Seu carinho e gentileza com todos colorem as páginas desse e-book. Nossa gratidão se estende a todos autores que fizeram desse projeto algo maior do que havíamos previsto para ele.

Que este e-book seja uma fonte contínua de conhecimento e inspiração, reforçando nosso compromisso com a proteção de dados e a construção de uma cultura de privacidade no Brasil.

Muito obrigado a todos!